
PRIVACY & INFORMATION MANAGEMENT
PIMtoolkit

TABLE OF CONTENTS

Guidelines for the Stage of Implementation - Self-Assessment Activity

PURPOSE

This tool is for the use of school board/authority members to identify where on the continuum their department/school or board/authority is with respect to each of the program elements identified through the PIM Toolkit.

Note: It is suggested that participants read the referenced documents prior to undertaking the self-assessment in order to gain an understanding of the expectations of the categories and, therefore, to have a context for the self-assessment activity.

Process Protocol

1. Start by having each team member independently identify (by placing a dot using a coloured marker) where on the team continuum the department/school or system is with respect to each of the program elements identified down the far left column.
2. Have participating team members independently provide an example of evidence to support their stage selection in each of the blank boxes corresponding to the program element and stage selected.
3. Next, have each participant transfer his/her stage selection to the Team Self-Assessment Activity Template. Post the sheet on a wall or centre on the table for a group review. The markers allow all team members to see how much they are in agreement with one another.
4. When all dots/marks have been placed on the team continuum, have team members reflect/brainstorm on where there is agreement or disagreement among the ratings.
5. Start with the first principle element and have team members discuss why they believe the department/school/system is where they rated it. Have team members continue this discussion until the team comes to a consensus on one stage that reflects where the department/school/ system is right now.
6. Have team members brainstorm on possible next steps for moving toward the next stage along the continuum.

SELF-ASSESSMENT ACTIVITY

Program Elements	Pre-Implementation Level 1 The system has not yet begun to address the program element.	Early Implementation Level 2 An effort has been made to address the program element, but the effort has not yet begun to impact a "critical mass."	Building Capacity Level 3 A critical mass has endorsed the program element. Members are beginning to modify their thinking and practice as they attempt to implement the program element.	Sustaining Capacity Level 4 The program element is deeply embedded in the system's culture. It represents a driving force in the daily work of the system. It is so internalized that it can survive changes in key personnel.
Foundational Program Elements				
Privacy Standard The privacy standard helps to foster a culture of privacy with respect to the way Ontario school boards/authorities collect, use, disclose, secure, retain, and dispose of personal information.				
Record and Information Management Framework The record and information management framework establishes a vision, goals, objectives, principles, and practices which are guided by legislation, policies, standards, and guidelines to support effective information management in school boards.				

SELF-ASSESSMENT ACTIVITY

Program Elements	Pre-Implementation Level 1 The system has not yet begun to address the program element.	Early Implementation Level 2 An effort has been made to address the program element, but the effort has not yet begun to impact a "critical mass."	Building Capacity Level 3 A critical mass has endorsed the program element. Members are beginning to modify their thinking and practice as they attempt to implement the program element.	Sustaining Capacity Level 4 The program element is deeply embedded in the system's culture. It represents a driving force in the daily work of the system. It is so internalized that it can survive changes in key personnel.
Data and Information Management				
Privacy Policy A written declaration that spells out the details of a school board's/authority's policy on the type of personal information it collects, how it uses that information, and how the information can be shared with third parties.				
Access and Control The access and control matrices are frameworks that will guide boards in their journey to identify, inventory, understand, and manage the requirements for access to personal information and personal information banks in support of the varied roles and duties within the organization.				

SELF-ASSESSMENT ACTIVITY

Program Elements	Pre-Implementation Level 1 The system has not yet begun to address the program element.	Early Implementation Level 2 An effort has been made to address the program element, but the effort has not yet begun to impact a "critical mass."	Building Capacity Level 3 A critical mass has endorsed the program element. Members are beginning to modify their thinking and practice as they attempt to implement the program element.	Sustaining Capacity Level 4 The program element is deeply embedded in the system's culture. It represents a driving force in the daily work of the system. It is so internalized that it can survive changes in key personnel.

Data and Information Management (cont'd)

Model Classification Scheme and Retention Schedule The model classification scheme and retention schedule is intended to provide a recommended classification methodology, legal citation table of retention periods, and recommended retention guidelines for school board/authority recorded information.				
Electronic Documents and Records Management System The electronic information landscape is growing rapidly – school boards/authorities need to consider effective ways to manage electronic documents and records.				

SELF-ASSESSMENT ACTIVITY

Program Elements	Pre-Implementation Level 1 The system has not yet begun to address the program element.	Early Implementation Level 2 An effort has been made to address the program element, but the effort has not yet begun to impact a "critical mass."	Building Capacity Level 3 A critical mass has endorsed the program element. Members are beginning to modify their thinking and practice as they attempt to implement the program element.	Sustaining Capacity Level 4 The program element is deeply embedded in the system's culture. It represents a driving force in the daily work of the system. It is so internalized that it can survive changes in key personnel.
Information Protection/Operational Control				
Password Procedures In a school board/authority environment, it is not uncommon for most employees to have multiple passwords for access to email, voice mail, computer applications, and portals. Every school board/authority should have a password strategy in place as part of the overall security strategy.				
Privacy and Information Security Guidelines School boards/authorities should have a variety of policies and/or procedures to guide the identification of areas of risk and strategies for the development of in internal procedure or regulation (e.g., guidelines for working outside the office, for cross-panel sharing of student information, for the use of Privacy and Confidentiality agreements and website, for video surveillance, and for video conferencing guidelines).				

SELF-ASSESSMENT ACTIVITY

Program Elements	Pre-Implementation Level 1 The system has not yet begun to address the program element.	Early Implementation Level 2 An effort has been made to address the program element, but the effort has not yet begun to impact a "critical mass."	Building Capacity Level 3 A critical mass has endorsed the program element. Members are beginning to modify their thinking and practice as they attempt to implement the program element.	Sustaining Capacity Level 4 The program element is deeply embedded in the system's culture. It represents a driving force in the daily work of the system. It is so internalized that it can survive changes in key personnel.
Information Protection/Operational Control (cont'd)				
Data Encryption Encryption is a secure process for keeping personal and confidential information private. It is a process by which bits of data are mathematically jumbled using a password key. The encryption process makes the data unreadable unless or until decrypted.				
Information Technology Equipment Hardware Disposal and Redistribution Guidelines All school board/authority computer systems, electronic devices, and electronic storage media should be purged of sensitive personal or confidential data when it is no longer needed or before reuse of such equipment to ensure the continued protection of personal and corporate privacy.				

SELF-ASSESSMENT ACTIVITY

Program Elements	Pre-Implementation Level 1	Early Implementation Level 2	Building Capacity Level 3	Sustaining Capacity Level 4
	The system has not yet begun to address the program element.	An effort has been made to address the program element, but the effort has not yet begun to impact a "critical mass."	A critical mass has endorsed the program element. Members are beginning to modify their thinking and practice as they attempt to implement the program element.	The program element is deeply embedded in the system's culture. It represents a driving force in the daily work of the system. It is so internalized that it can survive changes in key personnel.

Risk Management

Privacy Impact Assessment (PIA) A PIA is an assessment framework used to identify the actual or potential risks that a proposed or existing information system, technology, or program may have on an individual's privacy.				
Privacy Breach Protocol The protocol is designed to help Ontario school boards/ authorities contain and respond to incidents involving unauthorized disclosure of personal information.				

SELF-ASSESSMENT ACTIVITY

Program Elements	Pre-Implementation Level 1 The system has not yet begun to address the program element.	Early Implementation Level 2 An effort has been made to address the program element, but the effort has not yet begun to impact a "critical mass."	Building Capacity Level 3 A critical mass has endorsed the program element. Members are beginning to modify their thinking and practice as they attempt to implement the program element.	Sustaining Capacity Level 4 The program element is deeply embedded in the system's culture. It represents a driving force in the daily work of the system. It is so internalized that it can survive changes in key personnel.
Risk Management (cont'd)				
Privacy Notification Privacy notification statements explain how personal information will be treated as individuals interact with a school board/authority or school. These statements assure both internal and external publics that the personal and confidential information they provide will be handled appropriately.				

PURPOSE

Ontario school boards/authorities should use this checklist as they feel appropriate as a means of gauging how aware staff are about protecting privacy. Staff should reflect upon their responses and act when they can. This is an awareness-enhancing exercise first.

Introduction

In accordance with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), *the Personal Health Information Protection Act* (PHIPA), and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), all Ontario school board/authority employees are responsible for the protection of personal, confidential, and sensitive information entrusted to them. They should be aware of privacy policies, procedures, and practices. Personal information is secured and protected from unauthorized access, disclosure, and inadvertent destruction by adhering to safeguards appropriate to the sensitivity of the information.

This tool is designed to raise your level of awareness of privacy issues. Do not hesitate to contact your school board's/authority's Freedom of Information Coordinator at telephone number _____ if you have any questions.

DO YOU FOLLOW YOUR PRIVACY POLICY AND/OR PROCEDURE?

A. Security of Personal, Confidential, or Sensitive Information	Yes	No	N/A
1. Are all hard copies of personal, confidential, or sensitive information stored in lockable filing cabinets?	☐	☐	☐
2. Have I safeguarded all electronic personal information records maintained in password-protected databases?	☐	☐	☐
3. Do I refrain from storing personal, confidential, or sensitive information on a Shared Network Drive?	☐	☐	☐
4. Do I immediately pick up any personal, confidential, or sensitive records sent to printer, photocopier or received by fax?	☐	☐	☐
5. If I notice personal, confidential, or sensitive information left at the printer/copier/fax machines, do I immediately retrieve them and/or return them to the owner?	☐	☐	☐
6. Before sending personal, confidential, or sensitive information via email, have I considered taking precautions such as removing personal information?	☐	☐	☐

	Yes	No	N/A
7. Have I considered alternatives to faxing personal, confidential, or sensitive information? If such information must be faxed, have the following precautions been taken:			
• Ensure that a fax cover sheet is used that contains contact information of both the sender and recipient with the mention "Confidential"?	☐	☐	☐
• Call the intended recipient immediately before and after sending the fax to ensure receipt and immediate pick-up?	☐	☐	☐
• Print and check a confirmation activity sheet to ensure that the fax reached its intended recipient?	☐	☐	☐
• Retrieve originals from the fax machine as soon as completed?	☐	☐	☐
8. If it is necessary to take information out of the office, have all necessary precautions been taken to ensure that it is protected? Is it possible to only take non-confidential/ sensitive information? If not, do I have managerial approval to take personal, confidential, or sensitive information from the workplace?	☐	☐	☐
9. Are computer access rights reviewed and updated regularly to ensure that I do not have access to personal information that I do not need to perform my duties and responsibilities?	☐	☐	☐
10. Am I following the procedures in place for safeguarding personal information on laptops, memory sticks, personal digital assistants (PDAs, e.g., BlackBerry devices), etc.?	☐	☐	☐

Comments:

B. Limitation of Collection, Use, Retention, and Disclosure of Personal Information	**Yes**	**No**	**N/A**
1. Do I need to collect, use, or disclose identifiable personal information to perform my duties and responsibilities?	☐	☐	☐
2. If I need identifiable personal information, do I need to obtain the consent of the individual to whom the information relates before collecting, using or disclosing their personal information?	☐	☐	☐
3. Do I limit my collection, use, or disclosure of personal information to only that which I require to perform my duties and responsibilities?	☐	☐	☐
4. Is there a clear purpose for each type of personal information that I collect, use, retain, or disclose?	☐	☐	☐

	Yes	No	N/A
5. Do I provide a notice to individuals whenever their personal information is collected, e.g., on forms, surveys, websites, etc.?	☐	☐	☐
6. Is all the personal information that I use or disclose utilized for the purpose for which it was collected, or for a consistent purpose?	☐	☐	☐
7. Do all notices of collection that I use provide the specific purposes of collection, the legal authority for collection, and the contact information for an official who can answer questions about the purposes of collection?	☐	☐	☐
8. Do I know who in my workplace is responsible for maintaining records retention schedules?	☐	☐	☐
9. Do I securely dispose of (i.e., destroy or store) personal, confidential, or sensitive information in accordance with established records retention schedules?	☐	☐	☐
10. Do I know when it is appropriate to destroy personal, confidential, or sensitive information? When destroying such information, do I place it in the appropriate shredding bins?	☐	☐	☐
11. Am I aware that all information stored in the memory of electronic devices (e.g., personal computers, printers, photocopiers, fax machines, etc.) has to be deleted permanently prior to their removal from the office?	☐	☐	☐

Comments:

C. Workstation Security	Yes	No	N/A
1. Am I using a password-protected screen saver and is it set to turn on after five minutes of inactivity?	☐	☐	☐
2. Do I always log off or sign out of applications I am not using, and close the browser window?	☐	☐	☐
3. Do I always shut down my computer at the end of the day?	☐	☐	☐
4. Have I positioned my monitor so that casual observers cannot view personal, confidential or sensitive information?	☐	☐	☐
5. Have I adopted a "clean desk" model so that no personal, confidential or sensitive information or material is left unsecured at my desk?	☐	☐	☐
6. Do I make a habit of checking that my desk drawers, filing cabinets, and/or door are locked when I leave for the day?	☐	☐	☐

Comments:

D. Accuracy	Yes	No	N/A
1. Am I following the procedures in place to update personal information to ensure that it is still accurate?	☐	☐	☐
2. Am I following the procedures in place so that individuals can update their own personal information so that it is still accurate?	☐	☐	☐
3. Am I following the procedures in place for informing third party service providers to whom personal information has been disclosed that the information has been updated?	☐	☐	☐
4. Do I note on the record if individuals have disputed the accuracy of their personal information, so that subsequent users of the personal information are aware of it?	☐	☐	☐

Comments:

E. Third-Party Service Providers	Yes	No	N/A
1. When personal information is shared with, or collected, used or disclosed by a third party service provider under an arrangement with the Ontario school board/authority, am I making sure that the provider follow its own privacy policies, procedures, and practices?	☐	☐	☐
2. Am I verifying that there is a written agreement in place with any third party service provider with which I am sharing personal information, or if the provider has permission to collect, use, or disclose personal information on behalf of the Ontario school board/authority?	☐	☐	☐
3. If the answer to the question above is "Yes," do I monitor compliance with any agreement with a third party service provider?	☐	☐	☐

Comments:

F. School and Classroom	Yes	No	N/A
1. Ontario Student Records (OSR) and Office Index Cards are securely stored in the main office of the school and are only accessible by authorized personnel in the main office of the school.	☐	☐	☐
2. School staff have received training and are aware of the Ontario School Board/ Authority's Privacy and Access to Information Policy.	☐	☐	☐
3. Teachers' and administrators' notes and other instruction-related information about students is secured in the classroom or office in the school.	☐	☐	☐

	Yes	No	N/A
4. Information about a student(s) is shared only with other staff in the school who are assigned to work with the student(s), and only as needed to improve the education of the student(s).	☐	☐	☐
5. Full names of students and other personal information and/or photographs do not appear on work displayed in the school, on websites and/or in newsletters.	☐	☐	☐
6. Information related to student(s) is shared outside the classroom for educational purposes only with consent or notification of parent(s) or guardian(s).	☐	☐	☐

Comments:

G. Privacy Breaches	Yes	No	N/A
1. I am aware of my obligation to immediately report a suspected or actual privacy breach to my supervisor and the school board's/authority's Freedom of Information Coordinator.	☐	☐	☐
2. I am aware of the Ontario school board/authority's "Responding to a Suspected Privacy Breach" protocol?	☐	☐	☐

Comments:

PURPOSE

Use this tool in conjunction with the Privacy Standard to assess which stage your school board/authority has achieved for each of the 10 commitments.

Commitments	Pre-Implementation	Early Implementation	Building Capacity	Sustaining Capacity
Privacy commitments are based on globally recognized fair information principles and are grounded in Ontario privacy legislation.	The system has not yet begun to address the standard.	An effort has been made to address the standard, but the effort has not yet begun to impact a "critical mass."	A critical mass has endorsed the standard. Members are beginning to modify their thinking and practice as they attempt to implement the standard.	The standard is deeply embedded in the system's culture. It represents a driving force in the daily work of the system. It is so internalized that it can survive changes in key personnel.
Accountability Personal information under our control has designated individual(s) who are accountable for the school board's/authority's compliance with privacy legislation.				
Identifying Purposes The purposes for which personal information is collected, used, retained, and disclosed, as well as for notifying individuals, is identified at or before the time the information is collected.				

Commitments	Pre-Implementation	Early Implementation	Building Capacity	Sustaining Capacity
Privacy commitments are based on globally recognized fair information principles and are grounded in Ontario privacy legislation.	The system has not yet begun to address the standard.	An effort has been made to address the standard, but the effort has not yet begun to impact a "critical mass".	A critical mass has endorsed the standard. Members are beginning to modify their thinking and practice as they attempt to implement the standard.	The standard is deeply embedded in the system's culture. It represents a driving force in the daily work of the system. It is so internalized that it can survive changes in key personnel.
Consent The knowledge or consent of the individual is obtained for the collection, use or disclosure of personal information, except when not required by law.				
Limiting Collection The collection of personal information is limited to that which is necessary for the purposes identified by the organization. Information is collected by fair and lawful means.				
Limiting Use, Disclosure and Retention Personal information shall not be used or disclosed for purposes other than those for which is was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes, or as required by law.				

Commitments	Pre-Implementation	Early Implementation	Building Capacity	Sustaining Capacity
Privacy commitments are based on globally recognized fair information principles and are grounded in Ontario privacy legislation.	The system has not yet begun to address the standard.	An effort has been made to address the standard, but the effort has not yet begun to impact a "critical mass".	A critical mass has endorsed the standard. Members are beginning to modify their thinking and practice as they attempt to implement the standard.	The standard is deeply embedded in the system's culture. It represents a driving force in the daily work of the system. It is so internalized that it can survive changes in key personnel.
Accuracy Personal information is as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes for which it is to be used.				
Safeguards Personal information is protected from unauthorized access, disclosure, and inadvertent destruction by adhering to safeguards appropriate to the sensitivity of the information.				
Openness Information about policies and practices relating to the management of personal information is made readily available to the public, including breach protocol.				

Commitments	Pre-Implementation	Early Implementation	Building Capacity	Sustaining Capacity
Privacy commitments are based on globally recognized fair information principles and are grounded in Ontario privacy legislation.	The system has not yet begun to address the standard.	An effort has been made to address the standard, but the effort has not yet begun to impact a "critical mass".	A critical mass has endorsed the standard. Members are beginning to modify their thinking and practice as they attempt to implement the standard.	The standard is deeply embedded in the system's culture. It represents a driving force in the daily work of the system. It is so internalized that it can survive changes in key personnel.
Individual Access Upon request, an individual is informed of the existence, use, and disclosure of his/her personal information and is given access to that information. An individual may challenge the accuracy and completeness of the information and request that it be amended as appropriate or have a letter of objection retained on file.				
Challenging Compliance An individual shall be able to address a challenge concerning compliance with the above tenets to the designated individual(s) accountable for compliance.				

PURPOSE

The Privacy Standard sets the foundation for all guidelines, policies and procedure within the toolkit. It is expected that this Privacy Standard will be used in its entirety and will not be rewritten or otherwise interpreted. The 10 commitments contained in the Privacy Standard are strong only as a unit and are not intended to be implemented separately.

Overview

Definition of a Standard

A standard is a set of rules, guidelines, and characteristics for activities or their results, which is provided for common and repeated use. It is typically established by consensus and is usually a collective work created by bringing together the experience and expertise of all interested parties and stakeholders.

Standards are designed to achieve optimal community benefits within a given context based on best practices and experience in a certain field such as science, technology, or management. With the objective of building confidence and acceptance by target users, a standard is expressed in recognizable language, and its adoption is voluntary. Sometimes a standard is made compulsory when laws or regulations refer to it and make it obligatory. Other times, a standard is given force by being recognized by an authoritative body.

Purpose of the Privacy Standard

The Privacy Standard aligns the commitments of Ontario school boards/authorities regarding privacy protection with what they actually do when managing personal information by:

- documenting what is done;
- performing to that documentation in a systematic way;
- ensuring that the process is effective—for example, results are achieved, monitored, and verified;
- extending the reach of the standard to third party service providers; and
- recording the results of the work, thereby enhancing trust.

In this way, the Privacy Standard helps to foster a culture of privacy with respect to how Ontario school boards/authorities collect, use, disclose, secure, retain, and dispose of personal information. It also ensures the right of individuals to have access to personal information about themselves and, as appropriate, to have it corrected.

Benefits of a Privacy Standard

The Privacy Standard has been developed by the Privacy Information Management taskforce for use by Ontario school boards/authorities. The ten commitments which make up the Privacy Standard have been adapted from the CSA Fair Information Privacy Principles. All Ontario school board/authority employees and students will benefit from a clear understanding of the Standard and the activities that support it and its guidelines. The Standard will also be useful for the parents, students, and other stakeholders to understand what measures are being taken to protect their personal information.

Considerations in Developing the Privacy Standard

During the development of this Standard, consideration was given to existing legislation that has direct and indirect impact on Ontario school boards/authorities regarding the collection, use, disclosure, retention, and disposal of personal information, such as the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), the *Personal Health Information Protection Act* (PHIPA), the *Education Act* (including the Ontario Student Record Guidelines), and the *Personal Information and Protection of Electronic Documents Act* (PIPEDA). In addition, this Standard attempts to meet public expectations regarding the protection of personal information.

Some Ontario school boards/authorities have developed and implemented policies and procedures relating to the collection and use of employee and student personal information. These documents should be reviewed to ensure compliance and consistency with this Privacy Standard.

Scope and Application of the Privacy Standard

For the purpose of this Standard, personal information includes personal health information except where otherwise noted.

Municipal Freedom of Information and Protection of Privacy Act

The Ontario government's Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) sets out requirements for municipal government institutions to follow in order to provide a right of access and a right of correction to recorded information under their custody or control and to protect personal information about individuals held by those institutions.

MFIPPA defines personal information as recorded information about an identifiable individual, including:

- **a.** Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation, or marital or family status of the individual;
- **b.** Information relating to the education or the medical, psychiatric, psychological, criminal, or employment history of the individual or information relating to financial transactions in which the individual has been involved;
- **c.** Any identifying number, symbol, or other particular assigned to the individual;
- **d.** The address, telephone number, fingerprints, or blood type of the individual;

e. The personal opinions or views of the individual, except if they relate to another individual;

f. Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;

g. The views or opinions of another individual about the individual; and

h. The individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

MFIPPA provides that its confidentiality provisions prevail over those of the Education Act. Consideration should be given to compliance with both MFIPPA and the Education Act where possible.

Personal Health Information Protection Act

In addition, Ontario school boards/authorities are impacted by the Personal Health Information Protection Act (PHIPA), the purposes of which are:

a. To establish rules for the collection, use, and disclosure of personal health information about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information while facilitating the effective provision of health care;

b. To provide individuals with a right of access to personal health information about themselves subject to limited and specific exceptions set out in this Act; and

c. To provide individuals with a right to require the correction or amendment of personal health information about themselves subject to limited and specific exceptions set out in the Act.

PHIPA defines "personal health information" as identifying information about an individual in oral or recorded form if the information:

a. relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family;

b. relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual;

c. is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual;

d. relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual;

e. relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance;

f. is the individual's health number; or

g. identifies an individual's substitute decision-maker.

Implementing the Privacy Standard

Ontario school boards/authorities should be prepared to inform individuals about the personal information they have about the individual in their custody or control and how they manage it. They should also be prepared to demonstrate that their record-keeping practices comply with MFIPPA and with other legislation and records/information management policies and practices, and should be able to answer questions or address concerns that individuals might have.

Ontario school boards/authorities should have a plan that makes the protection of personal information a priority. Such a plan should:

- establish overall accountability for privacy;
- ensure that reasonable resources are coordinated and made available to meet the plan timelines and deliverables;
- provide extensive security awareness and privacy training at all levels;
- demonstrate senior-level commitment;
- include privacy issues in the job performance process; and
- develop, monitor, and enforce privacy policies and procedures.

Ontario school boards/authorities should monitor:

- deficiencies in compliance with requirements of law and school board policy, and address them appropriately and quickly;
- third party service providers' compliance with their contractual privacy obligations by a variety of means, such as obtaining relevant management statements of compliance, conducting periodic audits, or obtaining service auditor reports; and
- the content and implementation of privacy obligations in service agreements and information-sharing arrangements through periodic review and discussion.

Ontario School Boards/Authorities Privacy Standard

Ontario school boards/authorities are committed to the protection of personal information under their control and to the individuals' right of privacy regarding personal information that is collected, used, disclosed, and retained in the school system. To this end, this Standard of privacy commitments is based on globally recognized fair information principles and is grounded in Ontario privacy legislation. Implementation is recommended for all Ontario school boards/authorities.

1. Accountability and Responsibility

Under the Municipal Freedom of Information and Protection of Privacy Act, the boards of trustees of Ontario school boards/authorities are responsible for personal information under their control and may designate an individual within their school board/authority who is accountable for compliance with privacy legislation.

Under the Personal Health Information Protection Act, health information custodians are responsible for personal health information and may designate an individual within their school board as an agent to assist with compliance with privacy legislation.

2. **Specified Purposes**
   The purposes for which personal information is collected are specified, and individuals are notified of the purposes at or before the time personal information is collected.

3. **Consent**
   An individual's informed consent is required for the collection, use, and disclosure of personal information, except where otherwise permitted by law.

4. **Limiting Collection**
   The collection of personal information is fair, lawful, and limited to that which is necessary for the specified purposes.

5. **Limiting Use, Retention, and Disclosure**
   The use, retention, and disclosure of personal information are limited to the specified purposes identified to the individual, except where otherwise permitted by law.

6. **Accuracy**
   Ontario school boards/authorities ensure that personal information is accurate, complete, and up-to-date in order to fulfill the specified purposes for its collection, use, disclosure, and retention.

7. **Security Safeguards**
   Personal information is secured and protected from unauthorized access, disclosure, and inadvertent destruction by adhering to safeguards appropriate to the sensitivity of the information.

8. **Openness and Transparency**
   Policies and practices relating to the management of personal information are made readily available to the public.

9. **Access and Correction**
   An individual has the right to access his/her personal information and will be given access to that information in accordance with privacy legislation, subject to any restrictions. An individual has the right to challenge the accuracy and completeness of the information and request that it be amended, as appropriate, or to have a letter/statement of disagreement retained on file. Any individual to whom the disclosure has been granted in the year preceding a correction has the right to be notified of the correction/statement. An individual is to be advised of any third party service provider requests for his/her personal information in accordance with privacy legislation.

10. **Compliance**
    An individual may address or challenge compliance with the above principles to the designated individual(s) accountable in each of the Ontario school boards/authorities.

Implementing the Privacy Standard

1. Accountability and Responsibility

Under the Municipal Freedom of Information and Protection of Privacy Act, the boards of trustees of Ontario school boards/authorities are responsible by law for personal information under their control and may designate an individual within their school board/authority who is accountable for compliance with privacy legislation.

Under Personal Health Information Protection Act, health information custodians are responsible for personal health information and may designate an individual within their school board as an agent to assist with compliance with privacy legislation.

Implementation

a. Accountability for the development and implementation of policies related to the protection of privacy resides with the Director of Education, who may further delegate responsibility for administration of the development of procedures and administration of the privacy policies and procedures to a designate.

b. All Ontario school board/authority employees are aware of privacy policies, procedures, and practices.

c. Procedures are in place to ensure that third party service providers who have custody of personal information on behalf of the Ontario school board/authority will be held accountable for the required protection of that information. Third party service providers are obliged to abide by the Ontario school board/authority privacy policies, procedures, and practices.

d. Procedures regarding accountability and responsibility are communicated to all employees.

Typical implementation activities include, but are not limited to, the following:

i. The identity of the individual(s) designated by the Ontario school board/authority to oversee compliance with the principles shall be made known upon request.

ii. Third party service provider agreements specify that they comply with Ontario privacy legislation.

iii. Ontario school boards/authorities should provide training opportunities for all employees that are relevant to their roles.

Additional Reference Guidelines

Guidelines for an Information Management Policy
Guidelines for the Use of Third Party Service Provider Agreements with Models
Guidelines for Dealing with Requests for Data from External Agencies

2. Specified Purposes

The purposes for which personal information is collected are specified, and individuals are notified of the purposes at or before the time personal information is collected.

Implementation

a. Personal information is collected for specified purposes in accordance with the legislation.

b. Procedures are in place to provide notice to the individual(s) identifying the purpose(s) for which the personal information is collected, used and/or disclosed. All notices must contain:

- the purposes for which the information is to be used or disclosed;
- the legal authority for the collection, for example, the statutory section(s) which authorize the collection; and
- the title, business telephone number, and business and email address of an employee who can answer questions about the collection.

c. Procedures are in place to ensure that third party service providers who collect, use, retain, and/or disclose personal information on behalf of Ontario school boards/authorities do so only for specified purposes, and provide notice to individuals stating the purpose(s) for which the personal information is collected, used, and/or disclosed.

d. Procedures' specified purposes are communicated to all employees.

Typical implementation activities include, but are not limited to, the following:

i. Identifying the purposes to the individual (s) for which personal information is collected at or before the time of collection allows Ontario school boards/authorities to determine the information they need.

ii. The identified purposes are specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon how the information is collected, this identification of purpose can be provided orally or in writing. An application form, for example, may give notice of the purposes.

iii. Exceptions to notice, which are otherwise permitted by law, such as where personal information is collected for the purposes of awarding scholarships, are communicated.

iv. Ontario school boards/authorities should monitor the implementation of the collection, use, disclosure, and destruction procedures by employees and third party service providers by conducting periodic checks and other measures.

v. Ontario school boards/authorities should provide training opportunities for all employees with respect to procedures regarding specified purposes.

Additional Reference Guidelines

Guidelines for an Information Management Policy
Guidelines for the Use of Third Party Service Provider Agreements with Models
Guidelines for Dealing with Requests for Data from External Agencies
Guidelines for Drafting Privacy Notification Statements

3. Consent

An individual's informed consent is required for the collection, use, and disclosure of personal information, except where otherwise permitted by law.

Implementation

a. Procedures are in place to obtain consent from individuals regarding the collection, use, and disclosure of their personal information as required.

b. Procedures are in place in order to outline any exceptions to securing consent in accordance with the legislation. For example, MFIPPA does not require the consent of the individual for collection when information is collected directly from the individual. Indirect collections may require consent if no other exemption applies. Collection of personal health information requires consent, if no other exemption applies.

c. Procedures are in place to ensure that third party service providers obtain consent from individuals regarding the collection, use, and disclosure of their personal information, as required.

d. Procedures regarding obtaining necessary consent are communicated to all employees.

Typical implementation activities include, but are not limited to, the following:

i. Typically, Ontario school boards/authorities will seek consent, if required, for the use or disclosure of personal information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an Ontario school board/authority wants to use information for a purpose not previously identified and not consistent with such purpose).

ii. Consent shall not be obtained through deception. The purposes for which consent is sought must be clear to the individual.

iii. Individuals can give consent in many ways, but the type or form of the consent is dependent upon the circumstances; for example:

- Explicit, written consent: An application form may be used to seek consent, inform the individual of the use that will be made of the information, and collect the information to be used. By completing and signing the form, the individual is giving consent to the collection and the specified uses.
- Implicit consent: A check-off box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third party service providers.
- Oral consent: Consent may be given orally when information is collected

iv. Subject to legal or contractual restrictions and reasonable notice, an individual may withdraw consent at any time. The Ontario school board/authority should inform the individual of the implications of such withdrawal.

v. Ontario school boards/authorities should monitor the implementation of the consent procedures by employees and third party service providers by conducting periodic checks and other measures.

vi. Ontario school boards/authorities should provide training opportunities for all employees with respect to procedures regarding consent.

Additional Reference Guidelines

Guidelines for an Information Management Policy
Guidelines for the Use of Third Party Service Provider Agreements with Models
Guidelines for Dealing with Requests for Data from External Agencies
Guidelines for Drafting Privacy Notification Statements
Ministry of Education Ontario School Record (OSR) Guideline

4. Limiting Collection

The collection of personal information is fair, lawful, and limited to that which is necessary for the specified purposes.

Implementation

a. Personal information is only collected when it is essential for providing for the education of students or the employment of Ontario school boards'/authorities' employees or as required and authorized by law.

b. Procedures are in place to ensure that third party service providers limit their collection of personal information in accordance with the legislation.

c. Procedures regarding limiting collection are communicated to all employees.

Typical implementation activities include, but are not limited to, the following:

i. The Ontario school boards/authorities should only collect information necessary for the purposes that have been identified.

ii. Ontario school boards/authorities should monitor the implementation of the collection procedures by employees and third party service providers by conducting periodic checks and other measures.

iii. Ontario school boards/authorities should provide training opportunities for all employees with respect to procedures regarding limiting collection.

Additional Reference Guidelines

Guidelines for an Information Management Policy
Guidelines for the Use of Third Party Service Provider Agreements with Models
Guidelines for Dealing with Requests for Data from External Agencies

5. Limiting Use, Retention, and Disclosure

The use, retention, and disclosure of personal information are limited to the specified purposes identified to the individual, except where otherwise permitted by law.

Implementation

a. Procedures are in place to ensure that personal information that has been collected is used, retained, and disclosed solely for the purpose(s) identified to the individual or for a consistent purpose, except where otherwise permitted by law.

b. Procedures are in place to ensure that third party service providers collect, use, retain, and disclose personal information solely for the purpose(s) identified to the individuals.

c. Procedures are in place to ensure that personal information should be securely destroyed after the retention period has expired.

d. Procedures regarding limiting use, retention, and disclosure are communicated to all employees.

Typical implementation activities include, but are not limited to, the following:

i. Use of a record refers to access being made by employees in the program area of the Ontario school board/authority that holds the information. Privacy legislation restricts the use of personal information to the purpose for which it was collected; a consistent purpose; purposes to which the individual consents; and other limited circumstances.

ii. Ontario school boards/authorities only retain records containing personal information in accordance with the Ontario school board/authority retention schedule and for the period stated in the privacy legislation.

iii. Disclosure of information means the release of information in a record to those other than employees in the program area of the Ontario school board/authority that holds the record, except where otherwise limited by the law. Section 33 of MFIPPA permits the disclosure of personal information only under certain conditions.

Ontario school boards/authorities should make an informed decision considering all relevant circumstances before disclosing the personal information. These considerations should include whether the disclosure is in the interest of the individual(s) and whether the disclosure is absolutely necessary for providing for the education of students or administering the employment of Ontario school boards/authorities employees. Consequently, disclosure of personal information is only provided to employees and third party service providers who require this information to perform their duties.

iv. When Ontario school boards/authorities receive requests for personal information from the Ministry of Education, other Ministries, other Ontario school boards/authorities, or private agencies, they should verify the legal authority for the disclosure.

v. Ontario school boards/authorities should monitor the implementation of their procedures limiting use, retention, and disclosure by employees and third party service providers by conducting periodic checks and other measures.

vi. Ontario school boards/authorities should provide training opportunities for all employees with respect to procedures regarding limiting use, retention, and disclosure.

Additional Reference Guidelines

Guidelines for an Information Management Policy
Guidelines for the Use of Third Party Service Provider Agreements with Models
Guidelines for Dealing with Requests for Data from External Agencies
Guidelines for the Secure Destruction of Data
Guidelines for the Destruction of Hardware
Model Classification and Retention Schedule

6. Accuracy

Ontario school boards/authorities ensure that personal information is accurate, complete, and up-to-date in order to fulfill the specified purposes for its collection, use, disclosure, and retention.

Implementation

a. Procedures are in place to ensure that personal information that is collected is accurate, complete, and current prior to using such information.

b. Procedures are in place to ensure that the personal information that third party service providers collect is accurate, complete, and current prior to using such information.

c. Procedures regarding accuracy are communicated to all employees.

Typical implementation activities include, but are not limited to, the following:

i. Information is sufficiently accurate, complete, and up-to-date to avoid inaccurate information being used in decision-making about the individual. Ontario school boards/authorities should not routinely update personal information but only in the context of its use:

- Record correction requests as they are made;
- Identify and transfer misdirected requests in a timely manner; and
- Communicate corrections to individuals.

ii. When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the Ontario school board/authority should amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third party service providers having access to the information in question.

iii. Ontario school boards/authorities should monitor the implementation of accurate recording of personal information by employees and third party service providers by conducting periodic checks, random checks, and other measures. Any inconsistencies should be addressed.

iv. Ontario school boards/authorities should provide training opportunities for all employees with respect to procedures regarding accurate recording of personal information.

Additional Reference Guidelines

Guidelines for an Information Management Policy
Guidelines for the Use of Third Party Service Provider Agreements with Models
Guidelines for Dealing with Requests for Data from External Agencies
Model Classification and Retention Schedule
Guidelines for the Use of Electronic Records as Official Records

7. Security Safeguards

Personal information is secured and protected from unauthorized access, disclosure, and inadvertent destruction by adhering to safeguards appropriate to the sensitivity of the information.

Implementation

a. The level and nature of access to personal information that is provided to users is based on sensitivity and is essential for providing for the education of students or the employment of Ontario school boards/authorities employees.

b. Ontario school boards/authorities should assign responsibility of privacy risk management to an employee who is aware of current privacy laws and legislation.

c. Procedures are in place to secure personal information from loss, misuse, unauthorized access or disclosure, and inadvertent or inappropriate destruction.

d. Procedures are in place to ensure that third party service providers secure personal information from loss, misuse, unauthorized access or disclosure, and inadvertent or inappropriate destruction.

e. Procedures regarding security safeguards are communicated to all employees.

Typical implementation activities include, but are not limited to, the following:

i. Access to personal information is limited only to authorized employees based upon their assigned roles and responsibilities. Users are authenticated, for example, by user name and password.

ii. Ontario school boards/authorities should protect personal information regardless of the format in which it is held. The security safeguards should protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.

iii. Methods of protection should include, but are not limited to:

- Physical measures, for example, locked filing cabinets, restricted access to offices, sign-in logs, limited distribution of reports containing personal information, securely disposing of confidential information (shredding), protecting personal information sent by courier or mail;
- Organizational measures—for example, security clearances, and limiting access to and ability to change personal information in hard copy and electronic form—that are restricted to authorized employees within the Ontario school board/authority and/or third party service providers contracted by the Ontario school board/authority;
- Technological measures—for example, passwords, firewalls, levels of encryption, and controls are ensured for remote access and when transmitting data/information via the internet, restricted access to system configuration, super user functionality, master passwords, and security devices—are put in place;

- Disaster recovery plans in case of destruction, accidental loss of personal information, a natural disaster; and
- Measures applicable to the use of personal information off-site.

iv. Ontario school boards/authorities should monitor the implementation of security safeguards and privacy risk management by employees and third party service providers by conducting periodic checks and other measures. Identified threats to safeguarding personal information should be addressed and alternate practices put in place.

v. Ontario school boards/authorities should provide training opportunities (in-services) for all employees with respect to procedures regarding security safeguards and privacy risk management.

Additional Reference Guidelines

Guidelines for an Information Management Policy
Guidelines for the Use of Third Party Service Provider Agreements with Models
Guidelines for Dealing with Requests for Data from External Agencies
Guidelines for the Secure Destruction of Data
Guidelines for Working Outside the Office
Guidelines for Use of School Board-Owned Portable/Mobile Devices
Guidelines for Data Encryption
Guidelines for School Board Websites
Guidelines for Video Surveillance
Guidelines for Video Conferencing
Guidelines for the Use of Passwords
Guidelines for the Destruction of Hardware

8. Openness and Transparency

Policies and practices relating to the management of personal information are made readily available to the public.

Implementation

a. Ontario school boards/authorities should promote their commitment to the appropriate management of personal information and continually seek opportunities to publicize their privacy policies, procedures, and practices.

b. Ontario school boards/authorities should assign responsibility for requests for personal information to a designated employee to ensure that they are handled expeditiously in accordance with the legislation and/or the Ontario school board's/authority's approved privacy policies, procedures, and practices.

c. Ontario school boards/authorities should have a Privacy Breach Protocol which is communicated to all employees and third party service providers.

d. Procedures regarding openness and transparency are communicated to all employees.

Typical implementation activities include, but are not limited to, the following:

i. Individuals should be able to acquire information about an Ontario school board's/authority's privacy policies and procedures without unreasonable effort. The information made available should include, but is not limited to:

- The name/title and address of the employee who is responsible for the Ontario school board's/authority's privacy policies and practices and to whom inquiries and complaints can be communicated;
- The means of gaining access to personal information held by the Ontario school board/authority;
- A description of the type of personal information held by the Ontario school board/authority, including a general account of its use;
- Brochures, pamphlets, flyers, websites, and any other communication vehicles explaining the Ontario school board's/authority's information privacy, including the Privacy Breach Protocol and managing personal information policies, procedures, and practices; and
- A listing of personal information that is made available to related organizations.

ii. Ontario school boards/authorities should identify and report new and inconsistent uses of and disclosures of personal information, including:

- revising notices of collection that are out of date or incorrect;
- assigning responsibility for the currency and accuracy of notices of collection;
- assigning responsibility for assembling information to be reported for
- publication in the personal information bank; and
- communicating inconsistency notification procedures to employees.

iii. Ontario school boards/authorities should monitor the implementation of openness and transparency by employees and third party service providers by conducting periodic checks, an annual review, discussions with employees, and other measures.

iv. Ontario school boards/authorities should provide training opportunities for all employees with respect to procedures regarding openness and transparency. Training opportunities outline responsibilities to ensure that a culture of openness and transparency is maintained regarding its privacy practices, including procedures to be followed in the event of a privacy breach.

Additional Reference Guidelines

Guidelines for an Information Management Policy
Guidelines for the Use of Third Party Service Provider Agreements with Models
Guidelines for Dealing with Requests for Data from External Agencies
Guidelines for Selecting and Implementing Electronic Document and Record Management Systems
Model Classification and Retention Schedule

9. Access and Correction

An individual has the right to access his/her personal information and will be given access to that information in accordance with privacy legislation, subject to any restrictions. An individual has the right to challenge the accuracy and completeness of the information and request that it be amended as appropriate or to have a letter/statement of disagreement retained on file. Any individual to whom the disclosure has been granted in the year preceding a correction has the right to be notified of the correction/statement. An individual is advised of any third party service provider requests for his/her personal information in accordance with privacy legislation.

Implementation

a. Procedures are in place to ensure that, upon request, individuals are informed if the Ontario school boards/authorities hold their personal information and that they are allowed to have access to this information.

b. Procedures are in place to respond to individuals' requests for access or correction to their personal information within a reasonable time and at minimal or no cost.

c. Procedures are in place to ensure that, upon request, individuals are informed if third party service providers hold their personal information and that they are allowed to have access to this information.

d. Procedures are in place to respond to individuals' requests for access or correction to their personal information of third party service providers within a reasonable time and at minimal or no cost.

e. Procedures regarding access and correction are communicated to all employees.

Typical implementation activities include, but are not limited to, the following:

i. Upon request, an Ontario school board/authority should inform an individual whether or not the Ontario school board/authority holds personal information about the individual and should allow the individual access to this information. The Ontario school board/authority should provide an account of the use that has been made or is being made of the information as well as an account of the third party service providers to whom the information has been disclosed.

ii. The requested information is provided or made available in a reasonably understandable form, for example, if the Ontario school board/authority uses abbreviations or codes to record information, an explanation is provided.

iii. In order to respond to a request for access, an individual may be required to Provide sufficient information to permit an Ontario school board/authority to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

iv. Where the Ontario school board/authority decides not to amend a record in response to a request for correction, the individual has the right to attach a statement of disagreement.

v. If requested, the Ontario school board/authority must notify anyone to whom the information has been disclosed in the preceding year of the correction and/or letter/statement of disagreement.

vi. In providing an account of third party service providers to whom it has disclosed personal information about the individual, the Ontario school board/authority should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the Ontario school board/authority should provide a list of organizations to which it may have disclosed information about the individual.

vii. The Ontario school board/authority should:

- record access requests when they are made;
- authenticate or confirm the authority of requesters;
- identify and manage the disclosure of records that incorporate third party service providers' personal information in accordance with the legislation.

viii. Ontario school boards/authorities should monitor the implementation of its access and correction procedures by employees and third party service providers by conducting periodic checks and other measures.

ix. Ontario school boards/authorities should provide training opportunities for all employees with respect to procedures regarding access and correction.

Additional Reference Guidelines

Guidelines for an Information Management Policy
Guidelines for the Use of Third Party Service Provider Agreements with Models
Guidelines for Dealing with Requests for Data from External Agencies
Guidelines for Selecting and Implementing Electronic Document and Record Management Systems
Model Classification and Retention Schedule
Ministry of Education Ontario Student Record (OSR) Guideline

10. Compliance

An individual may address or challenge compliance with the above principles to the designated individual(s) accountable in each of the Ontario school boards/authorities.

Implementation

a. Procedures are in place to receive and respond to inquiries or complaints related to the managing of personal information.

b. The Director of Education or designate is apprised of all complaints and their resolution.

c. Procedures are in place to ensure that third party service providers respond to inquiries or complaints of their managing of personal information, and should advise the Director of Education or designate of all complaints and their resolution.

d. Procedures regarding compliance are communicated to all employees.

Typical implementation activities include, but are not limited to, the following:

i. Ontario school boards/authorities should inform individuals who make inquiries or lodge complaints of the existence of relevant complaint mechanisms as set out in the MFIPPA and PHIPA, as applicable.

ii. The complaint process should be easily accessible and simple to use.

iii. All complaints should be investigated, and deficiencies in compliance with the legislation are to be reported in accordance with the Ontario school board/authority policy. If a complaint is found to be justified through either the internal or external complaint review process, the Ontario school board/authority should take appropriate measures, including, if necessary, amending its privacy policies and procedures.

iv. Ontario school boards/authorities should monitor the implementation of their compliance procedures by employees and third party service providers by conducting periodic checks and other measures.

v. Ontario school boards/authorities should provide training opportunities for all employees with respect to procedures regarding compliance.

Additional Reference Guidelines

Guidelines for an Information Management Policy
Guidelines for the Use of Third Party Service Provider Agreements with Models
Guidelines for Dealing with Requests for Data from External Agencies
Ministry of Education Ontario Student Record (OSR) Guidelines, 2000

References

AICA/CICA Privacy Framework 2003 (Revised March 22, 2004) (American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants)

ARMA Standards Development Process

Canadian Standards Association Privacy Code 2007
http://www.csa.ca/standards/privacy/Default.asp?language=English

Information and Privacy Commissioner/Ontario, Creation of a Global Privacy Standard 200

Government of Ontario - Information and Information Technology Security Directive and Information Security and Privacy Classification (ISPC) Policy 2005

Government of Ontario, Access and Privacy Office, Office of the Corporate Chief Strategist, Management Board Secretariat - Corporate Operating Policy on Internet Tracking Technologies 2004

Government of Ontario - Ontario Shared Services Privacy Review 2005

PURPOSE

Records and information are important strategic assets of an organization and, like other organizational assets (people, capital and technology), must be managed to maximize their value. Information includes records that are important for their content and as evidence of communication, decisions, actions, and history. Effective information management is critical to the operation of schools and school boards/authorities and is a part of every employee's responsibilities. This document sets out an information management framework that is meant to provide a disciplined consistent approach for the management of information assets.

Vision

The objective of records and information management (RIM) is to achieve efficient and effective records and information management to support program and service delivery; to foster informed decision making; to facilitate accountability, transparency, and collaboration; and to preserve and ensure access to information and records in accordance with the laws of Canada and Ontario and for the benefit of present and future generations.

What Is Records and Information Management (RIM)?

RIM involves identifying, planning, directing, controlling, and evaluating information assets to meet organizational goals and to deliver programs and services. Records are an important subset of information and they must be managed in a disciplined, consistent, and coordinated manner.

RIM helps to establish disciplined, consistent practices related to the planning, creation, capture or collection, organization, use, accessibility, dissemination, storage, protection, and disposition of school board/authority-recorded information assets. Technology is key for effective information management.

Why Is RIM Important?

Through establishment of an effective RIM program, school boards and authorities will improve programs and services for students, decision making, information sharing, and access to and use of information. Additionally, RIM will support the preservation of corporate memory and organizational history; accountability, public trust and confidence; the management of risks to information, operations and services; and the protection of information-thereby protecting staff and students.

Goals of the RIM Framework

Implementing the RIM framework will help ensure that school boards and authorities reach the following goals:

- Provide timely, relevant, and accurate RIM to support the provision of programs and services that best meet students' needs.;
- Support informed decision-making and policy development, and effective, efficient, and trustworthy program and service delivery;
- Support transparency and accountability;
- Support access to and privacy of information in accordance with legislation and policies;
- Capture and manage records of business decisions and transactions and maintain corporate memory; and
- Support access to information for legal purposes.

The RIM Framework

(Based on the Government of Alberta Information Management Framework)

Objective of a Records and Information Management Framework

1. To establish a consistent and coordinated approach to RIM by establishing policy, standards, practices, and tools that reflect organizational needs.
2. To adopt a RIM framework that supports organizational goals and objectives and supports student needs.
3. To establish processes that ensure that information is accurate, reliable, trustworthy, and authentic; has a context and is able to serve as evidence; and supports accountability.
4. To build staff awareness and understanding of and commitment to managing information assets and protecting privacy and confidentiality at all levels of the organization.
5. To improve control and security through providing audit trails of document activities, ensuring their use as reliable information assets.
6. To establish an integrated, organization-wide solution for managing electronic information.
7. To develop a staff training strategy and build RIM skills.
8. To develop and implement metadata standards to support the identification, location, and retrieval of information.
9. To develop a strategy for the long-term management (migration) and preservation of information assets.
10. To assess progress in improving the management of information in the organization.

RIM PRINCIPLES AND COMMITMENTS

Principle 1 - Accessibility

Information will be readily available and accessible for as long it is required.

- **a.** Information to support evidence of communications, actions, and decisions is routinely recorded and stored.
- **b.** Information is accessible to staff who require it in the performance of their duties and are authorized to access it.
- **c.** Information is shared across the organization and with social agencies in accordance with operational needs and statutory provisions.
- **d.** Information is managed throughout its life cycle regardless of format.
- **e.** Rules are established for the organization, storage, retrieval, and destruction of records.
- **f.** Plans and practices to actively make records available to the public are in place, and records are available to the public by request, subject to the statutory requirements.

Principle 2 - Accountability and Stewardship

Accountability for managing information in the custody and control of the organization is clearly defined, communicated and monitored.

- **a.** Accountability for creating a record of business decisions and transactions and for maintaining corporate memory is clearly established and monitored.
- **b.** Roles and responsibilities for staff are articulated and understood for all management of information activities.
- **c.** Core competencies relating to managing information are identified, and training is provided.
- **d.** Performance in managing information is managed and measured.

Principle 3 - Risk Management

Risks to information are managed and practices and processes are in place to protect information assets.

- **a.** Risks to records and information are identified and managed.
- **b.** Practices are in place to protect confidential, sensitive, and personal records and information from unauthorized collection, use, disclosure, or destruction.
- **c.** All records are managed to meet rules of evidence and legal discovery.
- **d.** Contractual arrangements include provisions for the protection and appropriate use of records and information to mitigate risks.
- **e.** Records and information are managed to support business continuity and recovery in the event of disaster.
- **f.** Records and information are managed to protect privacy and confidentiality.

Principle 4 - Usability and Quality Control

RIM meets the needs of staff and stakeholders. RIM is timely, accurate, reliable, and relevant, has integrity, and is easy to use.

- **a.** Processes are in place to ensure that RIM is accurate, timely, reliable, and easy to use.
- **b.** RIM use is planned and managed.
- **c.** Records and information are managed appropriately throughout its entire life cycle-creation, capture, and collection; organization; storage, access, and use; and disclosure and disposition (destruction or permanent retention).
- **d.** Plans are in place to leverage the value of RIM by combining it with RIM from other internal or external sources, in accordance with statutory provisions, to improve programs and services.

  Processes and technology supports are in place to ensure appropriate access to records and information and tracking of who has modified or accessed confidential records.

Principle 5 - Planning and Coordination

Coordinated planning for RIM is linked to organizational goals, objectives, and financial planning.

- **a.** RIM practices are included in all program planning.
- **b.** RIM is coordinated across the organization-schools and departments.
- **c.** RIM is planned to support continuous service and disaster recovery.
- **d.** RIM is integrated into succession plans to ensure the capture and maintenance of corporate history.

Principle 6 - Integration

The management of records and information is integrated with program planning and other business processes.

- **a.** RIM practices are a component of program and project management.
- **b.** RIM is integrated across the organization (schools and departments) to support organizational objectives.

Legislation, Policies Standards and Practices

The context for records and information management for school boards/authorities is provided by legislation, Ministry Policy Program Memoranda, and school board/authority policies and procedures. School boards/authorities should be aware of the following statutes which provide guidance for the collection, use and maintenance of recorded information.

- ***The Education Act of Ontario***
  The Education Act is the administrative statute under which all Ontario school boards/authorities must operate. The Act sets out provisions for the creation and maintenance the pupil record (s. 265 (1) and s.266) and for the establishment of a records management program (s.171(38)).
- ***The Ontario Evidence Act***
  Sets out how RIM may be used as evidence in legal proceedings in a court of Ontario.
- ***The Canada Evidence Act***
  Sets out how RIM may be used as evidence in legal proceedings in a court in a matter under federal jurisdiction.
- ***The Municipal Freedom of Information and Protection of Privacy Act*** **(MFIPPA)**
  MFIPPA addresses issues of disclosure of records under the care and custody of school boards/authorities, as well as the collection, use, and disclosure of records containing personal information. MFIPPA also regulates the collection, use, disclosure, and accuracy of personal information stored in records and creates a process for obtaining access to recorded information.
- ***The Personal Health Information Protection Act*** **(PHIPA)**
  PHIPA addresses the collection, use, disclosure, retention, and destruction of personal health information.

- **Other Statutory Provisions**
  The Table of Laws and Citations with Retention Requirements for school boards/authorities included as part of the Guideline on the Model Classification Scheme and Retention Schedule provides a listing of other statutory provisions contained in the laws of Canada and Ontario that may affect the creation and retention of school board/authority RIM.
- **Ministry Policy and Program Memoranda**
  Ministry of Education PPM's may include requirements for the collection, creation, use retention and destruction of records and information.

Standards, Policies, Procedures and Practices

School boards/authorities will need to develop supporting policies, procedures, and guidelines for the completion of the RIM framework. Policies and procedures may include, but should not be limited to, the following:

- Information/records keeping policies management
- Classification and retention guidelines
- Guidelines for managing personal information and confidential information
- Guidelines for access and control of information
- Securing mobile devices
- Password management procedures
- Information architecture
- Records management guidelines

References

Government of Canada Information Management Framework

Government of Ontario Information Management Framework

Government of Alberta Information Management Framework

PURPOSE

Ontario school boards and authorities, like any other sector today, are struggling with huge volumes of paper and find themselves thinking more and more of electronic archiving and storage for records and documents. This guideline is intended to help direct and inform school boards/authorities in their decision making regarding electronic versus paper records

Overview

As more and more business is transacted and stored electronically, and imaging systems are installed to convert paper files to electronic form, the question arises about whether or not there is a need to print or maintain paper once the content is scanned. Retention periods, typically applied in the past to paper records, must now be applied to electronic records.

The issue does not have a quick resolution, nor is one statement necessarily applicable to all records. Consideration must be given to:

- the laws under which the school boards/authorities operate;
- laws which surround the types of records that are created and maintained;
- specific guidance from industry specialists (such as psychologists and health care professionals); and
- the policies and procedures implemented by the school board/authority and schools to manage the records and the systems used to create and store them.

Legislative Considerations

From the perspective of the school boards/authorities, several pieces of legislation apply:

- The Evidence Act for Ontario, which determines whether or not electronic records are admissible in court, defines what is required to prove the integrity of a record. It also references standards which may be used to determine admissibility. The Evidence Act can be found at http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90e23_e.htm.
- The Electronic Commerce Act of 2000 defines the requirements for using electronic records in place of paper and provides guidance on where and how electronic records can replace paper. The Electronic Commerce Act can be found at http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_00e17_e.htm.

Definitions

1. (1) In this Act,

"electronic" includes created, recorded, transmitted or stored in digital form or in other intangible form by electronic, magnetic or optical means or by any other means that has capabilities for creation, recording, transmission or storage similar to those means and "electronically" has a corresponding meaning ("électronique", "par voie électronique");

"electronic agent" means a computer program or any other electronic means used to initiate an act or to respond to electronic documents or acts, in whole or in part, without review by an individual at the time of the response or act ("agent électronique");

"electronic signature" means electronic information that a person creates or adopts in order to sign a document and that is in, attached to or associated with the document ("signature électronique");

"public body" means

(a) any ministry, agency, board, commission or other body of the Government of Ontario,

(b) a municipality or its local board, or

(c) an entity that is designated as a public body by a regulation made under clause 32(a) ("organisme public") 2000, c. 17, s. 1 (1).

In addition to these broad pieces of legislation, other laws and industry guidelines also impact the decision to retain electronic records in place of paper.

The Ministry of Education has issued its Instructions for the Use of Computerized Enrolment Registers for Elementary and Secondary Schools for the 2007–2008 year. In it, the guidelines state that:

School boards are no longer required to seek ministry approval to use computerized enrolment-recording systems instead of the ministry's registers. When board staff are satisfied that their computerized enrolment-recording system meets ministry requirements, their schools are no longer required to use the enrolment registers issued by the ministry. Ministry staff are available to provide advice during the board's implementation of a computerized system. However, school boards remain responsible for ensuring that their computerized enrolment-recording systems provide accurate data and satisfy all ministry requirements. These records must also be retained for the required length of time for ministry audit purposes.

(see "Retention of Pupil Enrolment Records" on page 2).

The Ontario Student Record Guideline adds another piece of complexity to the review in its requirement to maintain paper copies of records in the file for such records as report cards, despite their being created electronically for ease of use:

3.2 Report Cards: 3.2.1.4 Electronic format

School boards may use an electronic format of the Provincial Report Card, Grades 1–8, to facilitate completion and use. However, a completed Provincial Report Card, Grades 1–8, or an exact copy of the report card, must be filed in the OSR as a hard copy.

The same principle applies to the Ontario Student Transcript:

> ***3.3 The Ontario Student Transcript (OST)***
>
> The requirements for the OST are outlined in the Ontario Student Transcript (OST): Manual, 1999. Beginning with the 1999–2000 school year, the OST will be a cumulative and continuous record of a student's successful completion of Grade 9 and 10 courses, successful and unsuccessful attempts at completing Grade 11 and 12 courses and Ontario Academic Courses, and completion of other diploma requirements. The OST is part of the OSR. When it is maintained as a hard copy, it should be filed in the OSR folder. When it is maintained electronically, a hard copy must be produced and maintained in accordance with the Ontario Student Transcript (OST): Manual, 1999. For a sample of the OST form, see appendix C to this guideline.

Based on these requirements, it is necessary to assess whether or not all the records to be maintained in the OSR must be in hard copy. On the basis of this initial review, it would appear that that is the case. Therefore, even if electronic versions of records are acceptable to meet other requirements, such as the Evidence Act or electronic transactions acts, the Ministry guidelines for certain types of records may preclude reliance on electronic versions.

The Personal Health Information Protection Act, S.O. 2004, requires that health information custodians who use electronic means to collect, use, modify, disclose, retain or dispose of personal health information to complete with the prescribed requirements. See Ontario Regulation made under the PHIPA, 329/04.

Supporting Standards

Two key standards provide guidance for school boards on microfilm and imaging and on electronic records. Developed by the Canadian General Standards Board, these standards, explain how school boards can set up their policies, procedures, and related systems to meet the need for integrity, reliability, and trustworthiness. While designed to specifically support evidentiary requirements, the practices outlined in the standards support an electronic record-keeping framework within the school board in terms of good practice.

Summary

Unfortunately, the answer to the question of whether electronic records can replace paper is not a simple one and may vary depending on the specific records. Electronic records are legal. The question of whether they can replace paper will depend on review of the various pieces of legislation for which the records must be maintained.

Where electronic records can be maintained in place of paper, clearly defined policies and procedure should be in place.

To determine whether or not paper is required, several actions must be taken:

1. Establish electronic records policies and procedures, based on the CGSB standard "Electronic Records as Documentary Evidence."
2. Determine which records are currently a priority to convert to or maintain electronically.
3. Identify the legislation and/or guidelines which govern the creation and management of the records.
4. Determine whether or not there is a requirement to maintain a paper copy, and why.
5. Discuss the risk of not maintaining a paper copy with business owners, Records and Information Managers, Legal, and Information Technology staff..

PURPOSE

The purpose of the Records and Information Management (RIM) policy is to support the management of records and information in a disciplined, coordinated and strategic manner.

Policy Statement

The objective of the RIM program is to support efficient and effective program and service delivery; to foster informed decision making; to facilitate accountability, transparency, and collaboration; and to preserve and ensure access to records and information in accordance with the laws of Canada and Ontario and for the benefit of present and future generations.

Rationale

The (name of school board/authority) is committed to instituting and maintaining a comprehensive RIM program for the systematic creation of records and information that are accurate, authentic, reliable, trustworthy, support accountability, and are able to serve as evidence. Records and information shall be safely and securely maintained for as long as they are required and staff shall be trained on their responsibilities with regard to board records.

The school board/authority operates under the authority of the Education Act and its associated regulations. The creation and management of school board/authority records shall be in accordance with the provisions of the Education Act, the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), the school board/authority privacy policy, and other relevant statutes and regulations of the Province of Ontario and the Government of Canada.

RIM Principles

The RIM program shall be established in accordance with the following principles.

Accessibility: Records and information will be readily available and accessible to those who need it when they need it.

Accountability and Stewardship: Accountability for managing records and information in the custody and control of the organization is clearly defined, communicated, and monitored.

Risk Management: Risks to records and information are managed, and practices and processes are in place to protect information assets.

Usability and Quality Control: Records and information meets the needs of staff and stakeholders. Information is timely, accurate, reliable, relevant, has integrity, and is easy to use.

Planning and Coordination: Coordinated planning for records and information management is linked to organizational goals, objectives, and financial planning.

Integration: The management of records and information is integrated with program planning and other business processes.

Scope

This policy applies to all records within the custody or under the control of the school board/authority and addresses all aspects of school board/authority operations and all records made or received in the day-to-day business operations of the school or school board/authority, regardless of the medium in which those records are stored and maintained. It ensures that records are available as evidence of school board/authority functions and activities and supports operating requirements.

- It applies to all business applications and information technology systems used to create, store, and manage records and information including email, database applications, and websites.
- All records and information received, created, and maintained within the departments and schools support the day-to day-operations of the school/school board/authority and, as such, are the property of the school/school board/authority and are subject to this policy.
- Employees are responsible and accountable for creating and maintaining accurate records of their activities in accordance with the school board's/authority's RIM program.
- This policy applies to all school board/authority staff and to third party contractors or agents who collect or receive records and information on behalf of the school board/authority.

Responsibilities

All school board/authority employees are responsible for the records and information they create and maintain to support the business operations of the school/school board/authority. They must be aware of the policy and its requirements and ensure ongoing compliance with it.

This policy and its guidelines and procedures apply to all records and information within the custody or under the control of the school/school board/authority, including those records and information relating to the operation and administration of the school/school board/authority and those records and information relating to employees and students individually.

Each department within school or school board/authority must support the RIM program by ensuring that the policies and procedures are applied, and must also:

- Create, receive, and manage school board/authority records and information to provide details about and evidence of the activities of the school board/authority.
- Manage all records and information regardless of format (paper, electronic, audio, videotapes, etc.) according to applicable federal and Ontario laws and school board/authority by-laws and procedures.
- Manage electronic records and information, including email records, in the school board's/authority's content/records management application when feasible.
- Print and file records and information in the departmental records area if there is no electronic content/records management system in place.

- Maintain records and information according to the department file plan developed from the school board/authority classification scheme.
- Ensure that appropriate access and security rules are in place to protect both paper and electronic records as required.
- Apply the records and information retention schedules and securely dispose of records in accordance with those schedules.
- Ensure that all third party organizations, contractors, or agents who receive or collect personal information on behalf of the school board/authority are aware of and comply with this policy.

Administrative Procedures

The Director of Education is authorized to provide the administrative procedures necessary to implement this policy. This policy is subject to regular review.

PURPOSE

The purpose of using the Access Matrix is to ensure that your school board/authority is complying with the following requirements of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

1. *Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.*
2. *Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.*
3. *Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.*

MFIPPA O. Reg. 823 s.3/MFIPPA O. Reg. 460 s.4

The Access and Control matrices are frameworks that guide school boards/authorities in their journey to identify, inventory, understand, and manage the requirements for access to personal information and personal information banks in support of the varied roles and duties within the organization.

The matrix accomplishes two very important objectives: First, all typical school board/authority positions (roles) have all their data needs identified to ensure that the right information is made available to support the expectations of their day-to-day activities; and, second, it identifies areas of data security required to ensure that matters of personal privacy are documented and provided. The matrix framework provided does not represent a final outcome, but is intended to provide guidance in two areas: first, an organization of "like types" reflecting the roles defined within your school board/authority; and, second, to organize specific personal data inventories that are required to support the activities for your defined roles.

Overview

School boards/authorities manage a large variety of information. Advances in computer technology and online access have greatly improved our efficiency and effectiveness. These advances also present a serious challenge to achieving appropriate access and enough data security. Personal information needs to be protected against unauthorized disclosure; all of the information we store and refer to must be protected against accidental or deliberate modification or loss and must be available in a timely fashion. We must also establish and maintain its authenticity.

School boards/authorities should review access and security needs for the personal information under their control, undertaking the following actions:

- Ensure that inventories of personal information are complete and up-to-date.
- Document the access provided to personal information for each role in your organization.
  - Is the level of access provided in accordance with the day-to-day performance of the individual's duties?
  - Is the type of access provided appropriate to protect against accidental modification and/or deletion?
- Review access levels and make adjustments as necessary. This review should be done on a regular basis and as required to ensure continued effectiveness.

Using the Access and Control Matrices

The matrix defined here is a sample that can be used as a starting point for this exercise. The first two critical steps that must be completed are:

1. Define the roles at your board.
2. Customize an inventory of the information (data elements) that is accessed by the roles that have been defined.

The following factors were considered in building each matrix:

Legislation and regulations (e.g., Education Act, MFIPPA, PHIPA, CFSA, etc.)

- Level of access (e.g., own class, own school, own area, whole board)
  Note: each board/authority will need to decide its own level of access (see below)
- Personal Information "groups" as follows: student, employee, other (parent, vendor, trustee, etc.)
  Note: These big group columns may be further broken down into a number of subgroups (e.g., specialized elementary teacher may include French, music, art, or phys. ed. in a single school or a number of schools; and centralized/specialized roles may include program and special education consultants, speech and language pathologists, health support workers, and many others).
- The roles, tasks, and/or functions identified in the matrices relate only to access to PERSONAL INFORMATION.

The access and control matrices included outline the major roles within each school board/authority and typical data elements. Each matrix can be used as is or can be modified to suit a particular school board/authority. School boards/authorities should define their own information types (data elements) as well as the titles of their actual roles, tasks, and functions.

How to Fill in the Matrix

Note: It is highly recommended that multidisciplinary teams within your school board/authority complete this matrix to ensure the broadest insight into unique roles and that data needs are identified and mapped. As an example, teams could be broken down into an academic review team to examine the roles and data inventory requirements for the academic section, and an administrative review team could examine the administrative and business roles and data inventory requirements for the administrative section. How one chooses to select and segment the teams is up to individual school boards/authorities to decide.

Completing the matrix is a two-stage process. The first stage identifies the data and access needs of the role. The second stage evaluates the school board's/authority's abilities to provide the access required based on its technology, proceduresm and practices (tools and rules).

Stage One: Identifying the Needs

When completing the matrix, it is important to adopt the perspective of what access is required to perform the duties of each role. For each unique role defined within your school board/authority, assess the needs of the role(s) to access/modify the data elements within your defined data categories (matrices). During this needs assessment it will be necessary for you to define the access into two segments. First, assess the type of access, such as No Access, Read-Only Access, or Read/Write/Modify Access. Second, define the level of access to reflect data at the individual/student level, class level, school level and/or school board/authority level. You may define additional levels of access to include other common working or organizational groups used in your school board/authority, such as family of schools, etc.

When completing the matrix for the first time, try to avoid filtering the "needs" based on the capabilities of the "tools or rules" used by your board. In other words, do not get stuck thinking that "My software won't let me do that" or "That's not how things work here." The initial stage of this exercise requires you to examine the real data "needs" and is not yet concerned with how they are delivered within your board.

Stage Two: Alignment – Evaluation of the Needs

Once the matrix is completed, you will need to assess your "tools and rules" to determine how well the current capabilities of your data systems meet the data needs of the roles now defined.

It is unreasonable to expect that the needs requirements will fully align with your current tools and rules. You should pay attention to areas where the data needs are not supported well within your school board/authority. In each of these misaligned areas, you should examine the opportunities within your school board/authority to modify either:

a. your "tools" to provide the extended access as required; or

b. your "rules" for defining internal procedure(s) to permit staff to perform the role(s) as expected while protecting the privacy of all students and staff.

Defining Roles and Responsibilities

This section of the access matrix development for your school board/authority is critical. Each unique role within your school board's/authority's employment structure becomes a column within your matrix and needs to be represented here. Our sample matrix divides school boards/authorities into two groupings. The first represents academic roles within your system; the second represents administrative roles. These sample matrices are provided as an example only, and you will need to modify them in whatever way makes sense for defining groupings of common roles within your own board structure.

While our sample matrices include some roles that are self-evident, others represent types of roles that will need to be expanded within your Access matrix design—for example, the role of central or itinerant teachers in the Academic sample matrix. Each school board/authority has its own unique classifications for these individuals who either move between classrooms within the same school or may serve many students across many schools. Each of these unique roles must be identified as a column in the matrix so that its data needs can be assessed and defined. Similarly, you may have employment distinctions between different types of office support workers that will need to be broken out based on their unique job requirements. Our sample seeks only to provide you with an initial position and areas of thought for you to fill in based on your own school board's/authority's structures.

An area to pay particular attention to is roles involving health-related services. These roles are usually described as psychologists, psychiatrists, child/youth workers, etc. These individuals typically have several levels of privacy legislation pertaining to their roles within the school board/authority and may be governed by professional councils or colleges not contained within our typical governance. For this purpose, we have indicated their roles distinctly in the sample matrix and suggest that you take time to isolate your health care providers similarly to ensure adequate treatment of their additional legislative responsibilities.

While defining these roles is a very large task, it need not be overwhelming. A good place to begin is by examining existing organizational charts for administrative departments and examining typical school structures at both the elementary and secondary levels within your school board/authority. From there, have your committee representatives

examine how current the charts are and include any known new or upcoming employee roles. As a rule of thumb, when in doubt, include the role being examined as its own column. The point of consolidation for roles may become more apparent at the end of this exercise. For now, just make sure that the needs of the roles are captured first. It is also very important that you initially approach this exercise from the position of having no restrictions. Think first of the needs of your system and of whether there are roles currently defined within your school board/authority or not. Once the needs are identified, you may find some commonality across roles that might suggest other efficiencies for your school board/authority.

Defining Data Elements

Personal Information Groups

The personal information groups are the various types of data that staff will access. The information will be categorized differently from school board/authority to school board/authority; therefore, the definition of the data and grouping is critical to the development of the matrix for your individual school board/authority.

A number of factors must be considered when defining your personal information groups, such as specific privacy legislation that applies to the data and groups. For example, medical information or special education information may fall under the jurisdiction of different legislation than attendance information. If the various information groups are defined correctly, it will be easier to align them with the roles.

The sample matrix is grouped at the highest level by Student and Employment. The next level of groups is more specific and may be grouped by function or department; some examples include Demographic, Attendance, Payroll and Benefits, and Health and Safety. The third level should be the most specific level defined and consists of information or groups that are accessed by a specific role.

A number of sources can be referenced when defining personal information groups on the matrix. The information systems being used at your school board/authority have grouped information by screen and function. System documentation and reference manuals may be of assistance when defining information groups.

Review and revise the personal information groups as required. During the process of aligning the information to the roles, it will be necessary to make modifications as various scenarios are worked through.

Types of Access

School boards/authorities need to establish their own type of access for each piece of personal information data.

Example:

RO: Read Only	The user has the ability to read data but not add, delete or edit.
RW: Read/Write	The user has the ability to enter, change, update or delete data.
NA: No Access	The user may not access the data.

Levels of Access

School boards/authorities need to establish their own level of access for each piece of personal information data.

Example:

B: Board/authority level access	Access to this information element for the entire organization
C: Class level access	Access to this information element only as it applies to their class
S: School level access	Access to this information element for all students or staff in their entire school
I: Individual level access	Access to this information element for individual students or staff
D: Department level access	Access to this information element as it applies to their department

Description of the Matrices

Table 1

- Academic Users and Student Personal Information
- Academic Users and Employee Personal Information
- Academic Users and the Rest of the Personal Information Groups

Table 2

- Business Users and Student Personal Information
- Business Users and Employee Personal Information
- Business Users and the Rest of the Personal Information Groups

Relevant Legislation

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) R.S.O. 1990, C.M-56

Since 1991, school boards/authorities have had to work towards complying with MFIPPA. The Act, in very general terms, is about making as much information available publicly as possible without invading the privacy rights of individuals. All "banks" or holdings of personal information must follow the rules established in the legislation regarding how personal information is collected, how it is used, and how is it disclosed.

- **Collection:** While collection is strictly controlled by MFIPPA, it is not relevant in relation to the access matrices and will not be addressed in detail here.
- **Use:** Use generally refers to the sharing of personal information within the school board/authority proper. School boards/authorities are authorized to use personal information under the following circumstances:
  a. if the person to whom the information relates has identified that information in particular and consented to its use;
  b. for the purpose for which it was obtained or compiled or for a consistent purpose*;

(MFIPPA s. 31)

- Disclosure: Disclosure generally refers to the release of personal information outside of the school board/authority.
  School boards/authorities are authorized to disclose personal information under the following circumstances:

  a. in accordance with the access provisions within MFIPPA;

  b. if the person to whom the information relates has identified that information in particular and has consented to its disclosure;

  c. for the purpose for which it was obtained or compiled or for a consistent purpose*;

  d. if the disclosure is made to an officer, employee, consultant or agent of the institution who needs the record in the performance of their duties and if the disclosure is necessary and proper in the discharge of the institution's functions;

  e. for the purpose of complying with an Act of the Legislature or an Act of Parliament, an agreement or arrangement under such an Act or a treaty;

  f. to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty or legislative authority;

  g. if disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;

  h. in compelling circumstances affecting the health or safety of an individual if upon disclosure notification is mailed to the last known address of the individual to whom the information relates;

  i. in compassionate circumstances, to facilitate contact with the spouse, a close relative or a friend of an individual who is injured, ill or deceased;

  j. to the Minister (of Education);

  k. to the Information and Privacy Commissioner;

  l. to the Government of Canada or the Government of Ontario in order to facilitate the auditing of shared cost programs.

  (MFIPPA s. 32)

  A further step when contemplating disclosure is to consider whether the disclosure would constitute an unjustified invasion of privacy. All the relevant circumstances must be considered including whether the personal information is needed in a fair determination of rights affecting the person who made the request and if the personal information is highly sensitive. An example of an unjustified invasion of privacy would be the disclosure of employment or educational history.

  (MFIPPA)

- **Consistent Purpose:** When personal information is first collected, the purpose is explained to the individual. Later, if another purpose for the information (either an internal use or an external disclosure) can be determined to be consistent with the original description of how it would be used and if it is deemed that the individual might reasonably have expected such a use or disclosure, then you are able to use/disclose the personal information in the new way.

  (MFIPPA s. 33)

Further Considerations

MFIPPA prevails over a confidentiality provision in any other Act unless the other Act or this Act specifically provides otherwise. In other words, another Act would have to expressly state that the particular provision takes precedence over protection provisions in MFIPPA.

(MFIPPA s. 53 (1))

It is an offence under MFIPPA to willfully keep or disclose personal information in contravention of this Act. It is also an offence to make a request under this Act for access to or correction of personal information under false pretences; to willfully obstruct the Commissioner in the performance of his or her functions under this Act; to willfully make a false statement to mislead or attempt to mislead the Commissioner in the performance of his or her functions under this Act; or to willfully fail to comply with an order of the Commissioner.

Every person who commits such an offence and is convicted is liable to a fine not exceeding $5,000.

(MFIPPA s. 48)

Note Regarding Third Party Personal Information: *Third party personal information is personal information located in a record, document, file, etc. that relates predominantly to another individual. For example, if a teacher were to include his own personal information, such as cell phone number and weekend plans, in an email predominantly about a student and that email is filed in the student's OSR, then the teacher's information is third party personal information.*

If the transportation consortium is fully constituted as an independent organization, then it must be treated the same as any external organization and does not fall under the rules for MFIPPA.

Personal Health Information Protection Act (PHIPA)

In PHIPA, "personal health information" (PHI) is defined as identifying information about an individual in oral or recorded form, if the information:

- relates to the physical or mental health, including information regarding the health history of the individual's family;
- relates to the providing of health care, including the identification of a person as a provider of health care;
- is a plan of service within the meaning of the Long-Term Care Act, 1994;
- relates to payments or eligibility for health care;
- relates to the donation of any body part or bodily substance or is derived from the testing or examination of any such body part or bodily substance;
- is the health card number;
- identifies a substitute decision-maker [PHIPA, s. 4(1)].

Note: *PHI does not include identifying information in a record in the custody or under the control of a health information custodian if the record is maintained primarily for a purpose other than the provision of health care [PHIPA, s. 4(4)(b)].*

PHIPA is a consent-based law and so consent is required for the collection, use, and disclosure of PHI, subject to specific exceptions [PHIPA, s. 29]

Education Act

Pupil records

266. **(1)** In this section, except in subsection (12),

"record", in respect of a pupil, means a record under clause 265 (1) (d). 1991, c. 10, s. 7 (1); 2006, c. 10, s. 35 (1).

Pupil records privileged

(2) A record is privileged for the information and use of supervisory officers and the principal and teachers of the school for the improvement of instruction of the pupil, and such record

(a) subject to subsections (2.1), (3), (5), (5.1), (5.2) and (5.3), is not available to any other person; and without the written permission of the parent or guardian of the pupil or, where the pupil is an adult, the written permission of the pupil. R.S.O. 1990, c. E.2, s. 266 (2); 1991, c. 10, s. 7 (2); 2006, c. 10, s. 35 (2, 3).

Information to medical officer of health

(2.1) The principal of a school shall, upon request by the medical officer of health serving the area in which the school is located, give that medical officer of health the following information in respect of pupils enrolled in the school:

1. The pupil's name, address and telephone number.
2. The pupil's birthdate.
3. The name, address and telephone number of the pupil's parent or guardian. 1991, c. 10, s. 7 (3).

Right of parent and pupil

(3) A pupil, and his or her parent or guardian where the pupil is a minor, is entitled to examine the record of such pupil. R.S.O. 1990, c. E.2, s. 266 (3).

Information for Minister or board

(7) Nothing in this section prevents the compilation and delivery of such information as may be required by the Minister or by the board. R.S.O. 1990, c. E.2, s. 266 (7).

Secrecy re contents

(10) Except as permitted under this section, every person shall preserve secrecy in respect of the content of a record that comes to the person's knowledge in the course of his or her duties or employment, and no such person shall communicate any such knowledge to any other person except,

(a) as may be required in the performance of his or her duties; or

(b) with the written consent of the parent or guardian of the pupil where the pupil is a minor; or

(c) with the written consent of the pupil where the pupil is an adult. R.S.O. 1990, c. E.2, s. 266 (10).

Definition

(11) For the purposes of this section,

"guardian" includes a person, society or corporation who or that has custody of a pupil. R.S.O. 1990, c. E.2, s. 266 (11).

Use of record in disciplinary cases

(13) Nothing in this section prevents the use of a record in respect of a pupil by the principal of the school attended by the pupil or the board that operates the school for the purposes of a disciplinary proceeding instituted by the principal in respect of conduct for which the pupil is responsible to the principal. R.S.O. 1990, c. E.2, s. 266 (13).

Privacy re education numbers

266.3 (1) Except as permitted by this section or otherwise by law, no person shall collect, use, disclose or require the production of another person's Ontario education number. 1997, c. 31, s. 120.

Exception

(2) A prescribed educational or training institution may collect, use, disclose or require the production of a person's Ontario education number for purposes related to the provision of educational services to that person. 1997, c. 31, s. 120.

Same

(3) The Minister and a person or entity prescribed under clause 266.5 (1) (b) may collect, use or disclose or require the production of Ontario education numbers for purposes related to education administration, funding, planning or research. 1997, c. 31, s. 120; 2006, c. 10, s. 36.

Same

(4) The Minister and a prescribed educational or training institution may collect, use, disclose or require the production of a person's Ontario education number for purposes related to the provision of financial assistance associated with the person's education. 1997, c. 31, s. 120.

Offence

266.4 (1) Every person who contravenes subsection 266.3 (1) is guilty of an offence. 1997, c. 31, s. 120.

Penalty, individuals

(2) An individual who is convicted of an offence under this section is liable to a fine of not more than $5,000 or to imprisonment for a term of not more than six months, or to both. 1997, c. 31, s. 120.

Penalty, corporations

(3) A corporation that is convicted of an offence under this section is liable to a fine of not more than $25,000. 1997, c. 31, s. 120.

Definitions

- **Record** – "record" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes

  (a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof; and

  (b) subject to the regulations, any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution ("document").

  MFIPPA R.S.O. 1990, C.M-56 s.2.(1)

- **Personal Information** – "personal information" means recorded information about an identifiable individual, including

  (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;

  (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

  (c) any identifying number, symbol or other particular assigned to the individual;

  (d) the address, telephone number, fingerprints or blood type of the individual;

  (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;

  (g) the individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual ("renseignements personnels").

- **Personal Information Bank** – "personal information bank" means a collection of personal information that is organized and capable of being retrieved using an individual's name or an identifying number or particular assigned to the individual ("banque de renseignements personnels")

PURPOSE

The Education Act section 171 (1) 38 states that a board may:

"Institute a program of records management that will, subject to the regulations in respect of pupil records,

i. provide for the archival retention by the board or the Archivist of Ontario of school registers, minute books of the board and its predecessors, documents pertaining to boundaries of school sections, separate school zones and secondary school districts, original assessment and taxation records in the possession of the board and other records considered by the board to have enduring value or to be of historical interest, and

ii. establish, with the written approval of the auditor of the board, schedules for the retention, disposition and eventual destruction of records of the board and of the schools under its jurisdiction other than records retained for archival use; R.S.O. 1990, c. E.2, s. 171 (1), par. 38.

The Model School Board Classification and Retention Scheme is designed to help school boards comply with this provision of the Education Act and to meet its legal obligations with respect to records. It is intended as a framework for school boards/authorities that require an organization-wide records and information management program to enable them to efficiently and effectively manage their information resources."

This Model Classification and Retention Scheme is supported by the following documents:

- *This guideline which describes how the scheme should be used by school boards/authorities*
- *A Table of Laws of Canada and Ontario with Records Retention Requirements for School Boards/Authorities*
- *A Table of Legal Citations of Laws of Canada and Ontario with Records Retention Requirements for School Boards/Authorities*

Background

The model scheme includes recommended retention periods which are based on legal retention periods, best practices for records management, and operational needs. Normally, schedule retention periods reflect the minimum amount of time the records need to be kept to satisfy the requirements.

Schools boards/authorities will need to adapt the schedule to meet their local needs. This includes establishing an internal review and approval process for recommended retention periods to ensure the recommended retention satisfies school board/authority operational and litigation needs.

Schemes and schedules are "living" or "evergreen" documents and can not be considered "complete" at any point. Updates and revisions to both the nature of records retained and the retention periods applied to them continuously evolve. School boards/authorities need to ensure that their program is routinely reviewed and revised to accommodate these updates.

The Tables of Laws and Citations with Retention Requirements for School Boards/Authorities are current of September 2008. School boards/authorities with existing records management schemes and schedules programs may wish to review the tables to ensure that their program adheres to current legal retention requirements.

The School Board/Authortity Model Classification and Retention Schedule for School Board/Authority Records and Information

Classification

The model scheme is based on a functional classification methodology where records and information are classified in accordance with the functions and activities they support within the organization. Records and information are classified into eleven primary functional categories, as follows:

Function	Description
ADM	Administration
COM	Communications and Public Relations
FAC	Facilities Management
FIN	Finance
GOV	Governance and Policy
HUM	Human Resources
ICT	Information and Computer Technology
LEG	Legal
PDD	Program Development and Design
RPL	Research and Planning
STU	Student

Records Series

Like records with like retention periods are grouped together and grouped by the "function" they support in the organization. Records may support more than one function, and records series can be adjusted to other functions to support cultural considerations. The important thing is that staff know what records series the record belongs to and where they are classified. Scope notes describe what records are included in the records series. School boards/authorities may also choose to adjust records series to reflect cultural considerations.

Retention

- **Responsible Department Retention** - Each records series includes a recommended department to be responsible for managing the official record to ensure that responsibility for retaining the information is assigned. The department manager or superintendent is responsible for ensuring that the department meets its records obligations. In most cases, the responsible department will be the department that originates the record; however this should be determined by the local school board/authority.
- **Recommended Active Retention** - Recommends a period in which the information should be managed in the active office or desk area. This is generally based on the frequency with which the information is likely to be accessed, and the goal is to minimize the amount of record storage space required in the primary work area. As a general rule, if the records in a series are referred to more than once per month per linear foot, then they are considered to be active. If not, you may wish to consider moving them to an inactive storage area.
- **Recommended In-Active Retention** - Recommends a period in which recorded information may be moved to a designated storage area until the end of its retention period. Inactive retention includes near-line or off-line storage (see glossary). Records accessed less frequently than once per month per linear foot may be classed as inactive and moved to an inactive storage area. It important to note that inactive storage areas must be areas that allow for the protection and preservation of records, and must thus be free of the risk of mould or water damage.
- **Retention of Official Record** - The total retention period (active and inactive) for the official record.

Duplicates/Copies

In some cases, more than one department may need or use the records and information and for operational efficiency a department may choose to retain a copy or duplicate of the same record even if they are not responsible for maintaining the official record. The recommended retention of duplicate records recognizes that on occasions other departments will need to keep copies but sets a short term retention period of those copies to minimize duplication and maximize efficiencies. These duplicates or copies are subject to legal discovery and/or Freedom of Information Requests and should be minimized as much as possible. They must be controlled to reduce storage and handling costs and to support the integrity of a systematic records retention program.

Value of Recorded Information

Records series are assessed and assigned a recommended value as follows:

- **Vital Record** - Identifies records that are necessary to resume or continue operations and to recreate the company's legal and financial position in the event of a disaster.
- **Personal Information Bank (PIB)** - Identifies records that contain personal information and that should be included in a personal information bank listing in accordance with the Municipal Freedom of Information and Protection of Privacy Act.
- **Subject to Archival Selection** - Identifies records that may preserve history and may be of value for inclusion in archives. Where school boards do not have an official archive, consideration should be given to maintaining the records permanently.
- **Include in OSR** - Identifies records that may be included in the Ontario Student Record in accordance with the Ministry of Education OSR guideline and the applicable board procedure.

Reference

Notes provide a further explanation about the retention where necessary; for example, when the retention is based on an event, the event is explained for the records series, i.e., the event date is the date the record was created.

Legal Citation

Citations are included for the key Acts of Parliament, Statutory Instruments and any regulations deemed relevant to determining the retention periods for particular groups of records. The citation is cross-referenced to the School Board/Authority Table of Legal Retention Citations.

Understanding Retention Periods

The model classification scheme is based on best practice for managing records in school boards/authorities and emerging practices in the records management community. Where retention periods are defined in law, these are generally referenced and applied.

Where a retention period is not defined in law, a recommended retention period is applied which in many cases is based on an operating requirement and the record can be disposed of once the requirement has been satisfied. School boards/authorities must assess both the value of the record to their organization and the recommended retention period before adopting it for their organization.

To determine whether and how long records series should be maintained, the organization should consider the operational needs, costs, benefits, and risks involved. Retention decisions should be based on sound business practices and should allow for as much flexibility as possible within the existing legal, practical, and ethical constraints.

Understanding Limitations

A limitation is a period contained in law which specifies the period of time during which an individual or organization may sue or be sued after an event. Limitations are not retention periods, but are a legal consideration that must be part of the retention-setting process, particularly in the absence of a legally defined retention period. Identifying the relevant limitations is important because these define the scope and time frame of risk for the organization. Records retention under a litigation strategy would involve retaining records and information for the period set out in a Statute of Limitation, which may be longer than an operational need or legal retention. However, under the Limitations Act of Ontario, the start of the limitation period commences when the wronged party knows, or ought to know with reasonable diligence, the facts that underpin the cause of action. This makes it very difficult, if not impossible, to set a retention period based on a limitation.

To retain everything forever in the event of litigation is contrary to records and information management principles and defeats the objectives of a records management program. Organizations must balance the risk of litigation with the cost of managing, storing, and accessing records and information.

Legal Citations that Impact School Board/Authority Records and Information

Table I includes a list of key laws of Ontario and Canada that contain a prescribed retention or limitation period for school board/authority records.

Table II includes the specific section of the Act that references the prescribed retention or limitation period and includes the prescribed retention period for the record.

This document is useful for as a cross-reference for school boards with existing records management programs to ensure that their program adheres to current retention requirements.

Subject Listing

This is a list of subjects for records that school boards/authorities manage and the record series that each subject has been aligned with. This document is useful for cross-referencing records to records series and to help school boards/authorities develop departmental file plans.

Guideline for Determining What Records Need to be Retained

This document provides guidance on what constitutes a record and what records and information that school boards/authorities must retain.

Summary

The Model Classification and Retention Scheme has been developed to help school boards initiate a records management program of to update their existing program. School boards/authorities must adapt the model scheme and schedule to suit their school board's/authority's cultural, operational, and legal needs. The school board/authority scheme should be approved by the school board/authority, school board/authority legal counsel, and school board/authority auditor prior to implementation.

Updates and revisions to both the nature of records retained and the retention periods applied to them continuously evolve and school boards/authorities need to ensure that their scheme and schedule is routinely reviewed and revised.

PURPOSE

This table is a summary of key laws of Canada and Ontario applicable to school boards that contain records retention provisions as at September 3, 2008 to support a school board/authority records management program.

To review the law, click on the alpha code for the law or the law name and you will be redirected to the ServiceOntario e-laws or CanLII websites. For specific citations in the applicable law and required retention periods, see Table II.

Table I: Table of Statutes of Canada and Ontario with Records Retention Requirements for School Boards/Authorities

Alpha Code*	Statute
BCA-O	Building Code Act, 1992, S.O. 1992, c. 23
CPP-C	Canada Pension Plan, R.S.C. 1985, c. C-8
CAI-O	Compulsory Automobile Insurance Act, R.S.O. 1990, c. C.25
CA-C	Copyright Act, R.S.C. 1985, c. C-42
EA-O	Education Act R.S.O. 1990 c. E.2
ECA-0	Electronic Commerce Act, 2000, S.O. 2000, c. 17
EHTA-O	Employer Health Tax Act, R.S.O. 1990, c. E.11
EIA-C	Employment Insurance Act, S.C. 1996, c. 23
ESA-O	Employment Standards Act, 2000, S.O. 2000, c. 41
ETA-C	Excise Tax Act, R.S.C. 1985, c. E-15
FPPA-O	Fire Protection and Prevention Act, S.O. 1997, c. 4.
ITA-C	Income Tax Act, R.S.C. 1985, (5th Supp.) c. 1
ITA-O	Income Tax Act, R.S.O. 1990, c. I.2.
IA-O	Insurance Act, R.S.O. 1990, c. I.8.
LTTA-O	Land Transfer Tax Act, R.S.O. 1990, c. L.6
LA-O	Limitations Act, 2002, S.O. 2002, c. 24, Sch. B
MFIPPA-O	Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56.
OHSA-O	Occupational Health and Safety Act - R.R.O. 1990 R.S.O. 1990, c. 0.1.

Alpha Code*	Statute
PBA-O	Pension Benefits Act, R.S.O. 1990
PHIPA-O	Personal Health Information and Protection Act, 2004, c. 3, Sch. A.
RPLA-O	Real Property Limitations Act R.S.O. 1990, c. L.15
SDWA-O	Safe Drinking Water Act, 2002, S.O 2002, c. 32
TSSA-O	Technical Standards and Safety Act, 2000, S.O. 2000, c. 16.
WSIA-O	Workplace Safety and Insurance Act, 1997, S.O. 1997, c. 16, Sch. A

*Interpreting the Alpha Code	
Name of Law e.g., BCA - Building Code Act of Ontario	Statute of O - Ontario C - Canada

[1] e-laws is a database of Ontario statutes and regulations (consolidated and source law) maintained by the Ministry of the Attorney General. For more information, go to its website http://www.e-laws.gov.on.ca/index.html.

[1] CanLII is database of Federal and Provincial statutes and regulations managed by the Federation of Law Societies of Canada. For more information, go to http://www.canlii.org/.

Table II: Table of Legal Citations from Laws of Canada and Ontario with Records Retention Requirements for School Boards

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
BCA-O-1	Building Code Act, 1992, S.O. 1992, c. 23.	BCA-Os36 s. 36 1992, c. 23, s. 36	Building Code Act Offence - Limitation Period	Limitation period one year from time subject matter arose.
BCA-O02	Building Code Act, 1992, S.O. 1992, c. 23.	BCA-Os8 s. 8 1992, c. 23, s. 8 (1); 1997, c. 30, Sch. B, s. 7 (1).	Building Permit	Not specified. Building permits required for construction.
CPP-C-1	Canada Pension Plan, R.S.C. 1985, c. C-8	CPP-Cs24 s. 24(1) R.S., 1985, c. C-8, s. 24; 1991, c. 49, s. 207; 1997, c. 40, s. 64; 1998, c. 19, s. 253	Canada Pension Plan - Books and Records	C + 6 Retain books of account and all vouchers necessary to verify the information. If retained electronic must be readable for the full retention period.
CAIA-O-1	Compulsory Automobile Insurance Act, R.S.O. 1990, c. C.25	CAI-Os2(10) s. 2(10) R.S.O. 1990, c. C.25, s. 2 (10).	Automobile Insurance - Limitation	Limitation three years from the time the offence was committed or alleged to be committed.

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
CA-C-1	Copyright Act, R.S.C. 1985, c. C-42 Exception for Educational Institutions, Libraries, Archives and Museums Regulations, under the SOR/99-325	CA-CR325s5(3) s. 5(3) S.C. 1997, c. 24, s. 18(1)	Copies of Works - Requests	E + 3 (three years from when record was created)
CA-C-2	Copyright Act, R.S.C. 1985, c. C-42 Exception for Educational Institutions, Libraries, Archives and Museums Regulations, under the SOR/99-325	CA-CR325s4(3) s. 4(3)	Reproductions of Works	E + 3 (three years from when record was created)
CA-C-3	Copyright Act, R.S.C. 1985, c. C-42,	CA-Cs41 s. 41, R.S., 1985, c. C-42, s. 41; R.S., 1985, c. 10 (4th Supp.), s. 9; 1997, c. 24, s. 22	Copyright - Limitation for Civil Remedies	Limitation - three years from the time the plaintiff knew, could be reasonably expected to know or where the plaintiff could not reasonably be expected to know from the time they first knew.
CA-C-4	Copyright Act, R.S.C. 1985, c. C-42,	CA-Cs29.9(1) s. 29.9(1), as am. S.C. 1997, c. 24, s. 18(1)	Educational Institution News/ Telecommunication Copyright Records Records and marking	Not specified - retain a copy.
CA-C-5	Copyright Act, R.S.C. 1985, c. C-42, Educational Program, Work and Other Subject-matter Record-keeping Regulations, under the SOR/2001-296 See Schedule - Information Record Form	CA-Cs9 s. 9 S.C. 1997, c. 24, s. 18(1)	News Programs - Copies for Educational Use	Retain information record for two years after the copy of the work is destroyed.

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
EA-O-1	Education Act R.S.O. 1990 c. E.2	EA-Os198 s. 198(1)(a) R.S.O. 1990, c. E.2, s. 198 (1)	Board of Education Meeting Minutes	Permanent - Full and correct record of proceedings of every meeting.
EA-O-2	Education Act R.S.O. 1990 c. E.2	EA-Os218 s. 218 R.S.O. 1990, c. E.2, s. 218 (1); 1996, c. 32, s. 70 (5); 1997, c. 31, s. 111 (1); 2000, c. 11, s. 21.	Declaration of Vacant Seat - Limitation	Limitation - 90 days.
EA-O-3	Education Act R.S.O. 1990 c. E.2	EA-Os86 s. 86(5) R.S.O. 1990, c. E.2, s. 86 (5); 1997, c. 31, s. 52 (2).	Discontinued School Authority Records	Records shall be filed with the Ministry.
EA-O-4	Education Act R.S.O. 1990 c. E.2	EA-Os66(4) s. 66(4) R.S.O. 1990, c. E.2, s. 66 (4).	Dissolved Board of Education Records	Records to be forwarded to Ministry.
EA-O-5	Education Act R.S.O. 1990 c. E.2	EA-Os171(1)38 s. 171(1)38 R.S.O. 1990, c. E.2, s. 171 (1), par. 38.	Education Records Management/Archival Retention	Not specified. Authority to establish a program. Emphasis on boundaries, separate school zones and districts, original assessment and taxation records, and records considered by the board to be of enduring value or of historical value.
EA-O-6	Education Act R.S.O. 1990 c. E.2 Identification and Placement of Exceptional Pupils Regulation, under the O.R. 181/98	EA-OR181s8 s. 8 O. Reg. 181/98, s. 6 (8); O. Reg. 137/01, s. 1.	Individual Education Plans	File in OSR - retain according to OSR guideline.

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
EA-O-7	Education Act R.S.O. 1990 c. E.2 Ontario Student Record (OSR) Guideline, 2000	EA-OOSRs3.5	Office Index Card	E + 55 (event is transfer or retirement of student) Do not file in OSR.
EA-O-8	Education Act R.S.O. 1990 c. E.2 See - OSR Guideline	EA-Os265 s. 8 OSR Guideline	OSR - Retention, Storage, and Destruction of Information	E + 5 (event is retirement of student) Retain: • report cards • the documentation file, where applicable • additional information that is identified by the school board as appropriate for retention E + 55 (event is retirement of student) Retain: • OSR folder • OST • Office Index Card
EA-O-9	Education Act R.S.O. 1990 c. E.2 Ontario Regulation 99/02 Teacher Performance See also: Performance Appraisal of Experienced Teachers: Technical Requirements Manual	EA-OR99s9 s. 9 O. Reg. 264/06, s. 2	Performance Appraisals	E + 6 (event is six years from the date of the summative report of the performance appraisal)

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
EA-O-10	Education Act R.S.O. 1990 c. E.2 School Year and School Holidays Regulation under the, R.R.O. 1990, Reg. 304	EA-OR304s8 s. 8 R.P.O 1990, Reg. 304, s.8	Professional Activity Day Evaluations	Not specified. Retain on file.
EA-O-12	Education Act R.S.O. 1990 c. E.2	EA-Os265(n) s. 265(n) R.S.O. 1990, c. E.2, s. 265; 1991, c. 10, s. 6	School Visitors Book	Not specified.
EA-O-13	Education Act R.S.O. 1990 c. E.2 Special Education Programs and Services Regulation under the, R.R.O. 1990, Reg. 306	EA-OR306s6 s. 6 R.R.O 1990, Reg. 306, s.6	Special Education Plan	Maintain for review.
EA-O-14	Education Act, R.S.O. 1990, c. E.2 Collection of Personal Information, under the Education Act, O. Reg. 521/01	EA-OR521s2 s. 2 O. Reg. 521/01, s. 2 (2); O. Reg. 170/02, s. 1; O. Reg. 322/03, s. 1	Criminal Background Check - CBC	No retention specified.

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
EA-O-15	Education Act, R.S.O. 1990, c. E.2 Collection of Personal Information, under the Education Act, O. Reg. 521/01,	EA-OR521s2 s. 2 O. Reg. 521/01, s. 2 (2); O. Reg. 170/02, s. 1; O. Reg. 322/03, s. 1	Criminal Offence Declaration	No retention specified.
EA-O-16	Education Act, R.S.O. 1990, c. E.2 School Councils Regulation, under the Education Act, O.R. 612/00,	EA-OR612s16 s.16 O. Reg. 612/00, s. 16(1)	School Council Meeting Minutes/Financial Transactions	Four years for minutes. Financial Records to be retained for C + 6.
EA-0-17	Education Act, R.S.O. 1990, c. E.2 Violence Free Schools Policy - Ministry of Education 1994	EA-VFSP part V Part V 1994	Violent Incident Form	*Include in OSR E + 3 or E + 5 (as below) No Suspension/No Expulsion - E + 3 (where event is three years without report of a violent incident to police). Suspension: E + 3 (where event is completion of three consecutive years during which no further suspensions occurred for serious, violent behaviour). Expulsion: E + 5 (event is five years from the date of expulsion)

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
ECA-O-1	Electronic Commerce Act, 2000, S.O. 2000, c. 17,	ECA-Os12(2) s. 12(2) 2000, c. 17, s. 12(2)	Electronic Documents	Provides for retention of electronic document if the document is in original format or is one that accurately represents the information, if it is accessible and useable and where sent or received information identifies origin and destination (metadata).
ECA-O-2	Electronic Commerce Act, 2000, S.O. 2000, c. 17,	ECA-Os12(3) s. 12(3) 2000, c. 17, s. 12(1)	Electronic Documents - Previously Retained	Provides for retention of electronic documents prior to enactment of *Electronic Documents Act* (2000).
ECA-O-3	Electronic Commerce Act, 2000, S.O. 2000, c. 17,	ECA-Os12(1) s. 12(1) 2000, c. 17, s. 12(1)	Retention for Written Documents (Conversion of to Electronic)	Provides legal retention of written documents in electronic form.
EHTA-O-1	Employer Health Tax Act, R.S.O. 1990, c. E.11,	EHTA-Os12 s. 12 as am. S.O. 1994, c. 8, s. 13	Employer Health Tax Accounting Records	Permanent or until permission for their disposal is given by the Minister. Retain books of account and every primary source document required to verify the entries in Ontario.
EHTA-O-2	Employer Health Tax Act, R.S.O. 1990, c. E.11,	EHTA-Os37 s. 37 R.S.O. 1990, c. E.11, s. 12 (4); 1994, c.8, s. 13(4)	Employer Health Tax Act Offences - Limitation	E + 6 (event is the date on which the offence was, or is alleged to have been, committed)
EHTA-O-3	Employer Health Tax Act, R.S.O. 1990, c. E.11,	EHTA-Os6 s.6 as am. S.O. 1994, c. 8, s. 6(1); S.O. 2001, c. 23, s. 75	Employer Health Tax Refund - Limitation	E + 4 (event is the day on which the return was required to be delivered)

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
EHTA-O-4	Employer Health Tax Act, R.S.O. 1990, c. E.11,	ETHTA-Os8(1) s. 8(1) as am. S.O. 1994, c. 8, s. 8(1)	Health Tax - Limitation	E + 4 (event is the later of [1] the day on which the return was delivered or received by the Minister and [2] the day the return was required to be delivered)
EIA-C-1	Employment Insurance Act, S.C. 1996, c. 23, Employment Insurance Regulations, under the Employment Insurance Act, SOR/96-332,	EIA-CR332s19 s. 19 SOR/97-31, s. 10	Record of Employment	C + 6 - Employer's copy E + 1 - Employee's copy (event is when record completed)
EIA-C-2	Employment Insurance Act, S.C. 1996, c. 23,	EIA-Cs87 s. 87 as am. S.C. 1998, c. 19, s. 267	Books of Account	C + 6 In the event of an appeal, retain until the appeal is resolved.
EIA-C-3	Employment Insurance Act, S.C. 1996, c. 23,	EIA-Cs46 s. 46 1996, c.23, s. 46.1; 1999, c. 31, s. 77(F); 2004, c.25, ss. 133, 197	Directors Liability - Limitation	E + 6 (event is the occurrence of the act or omission for which the penalty is imposed)
EIA-C-4	Employment Insurance Act, S.C. 1996, c. 23,	EIA-Cs47(3) s. 47(3)	Employer Benefit Penalties - Limitation	E + 6 (event is the day on which the liability arose) Suspend if appeal or review pending.
EIA-C-5	Employment Insurance Act, S.C. 1996, c. 23,	EIA-Cs85(3) s. 85(3)	Employment Insurance Assessment - Limitation	C + 3

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
ESA-O-1	Employment Standards Act, 2000, S.O. 2000, c. 41,	ESA-Os15(8)&(9) s. 15(8)&(9) 2004, c. 21, s. 2	Agreements - Excess Hours and Averaging	E + 3 (event is last day work performed under the agreement)
ESA-O-2	Employment Standards Act, 2000, S.O. 2000, c. 41,	ESA-Os15 s. 15 2000, c. 41, s. 15 (1); 2002, c. 18, Sch. J, s. 3(6, 7)	Employee Records	E + 3 (event is the date employee ceased to be employed by employer). Includes: • employee's name and address • employee's date of birth, if the employee is a student and under 18 years of age, (retain three years after the employee's 18th birthday) • date on which the employee began his/her employment
ESA-O-3	Employment Standards Act, 2000, S.O. 2000, c. 41,	ESA-Os15(5)3 s.15(5) 3 2000, c. 41, s. 15 (5); 2002, c. 18, Sch. J, s. 3(8)	Employee Work Hours - Number of Hours Worked	E + 3 (event is the day worked) Includes number of hours worked in each day of each week.
ESA-O-4	Employment Standards Act, 2000, S.O. 2000, c. 41,	ESA-Os139 s. 139 2000, c. 41, s. 139	Employment Standards Act, 2000 Prosecution - Limitation	E + 2 (event is two years after the date on which the offence was committed or alleged to have been committed)
ESA-O-5	Employment Standards Act, 2000, S.O. 2000, c. 41,	ESA-Os15(7) s. 15(7) 2006, c. 13, s. 3 (1); 2007, c. 16, Sch. A, s. 2	Pregnancy/Parental/Emergency Leaves	E + 3 (event is the last day of leave)

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
ESA-O-6	Employment Standards Act, 2000, S.O. 2000, c. 41,	ESA-Os15.1(5) s. 15.1(5) 2002, c. 18, Sch. J, s. 3(9)	Vacation Pay Record	E + 3 (event is date record created) Includes number of hours worked in each day of each week.
ESA-O-7	Employment Standards Act, 2000, S.O. 2000, c. 41,	ESA-Os15(5)4 S15(5)4 2000, c. 41, s. 15 (5); 2002, c. 18, Sch. J, s. 3(8)	Wage Statements and Termination Pay	E + 3 (event is date information given to employee)
ETA-C-1	Excise Tax Act, R.S.C. 1985, c. E-15, See also Canada Revenue Agency GST/HST Memorada Series C. 15: Books and Records (Revised June 2005)	ETA-Cs286(3) s. 286(3)	GST Accounting	C + 6
ETA-C-2	Excise Tax Act, R.S.C. 1985, c. E-15, See also Canada Revenue Agency GST/HST Memorada Series C. 15: Books and Records (Revised June 2005)	ETA-Cs286(3.1) s. 286(3)	GST Electronic Records	C + 6 Records maintained electronically shall be kept in electronically readably format for the retention period.
FPPA-O-1	Fire Protection and Prevention Act, 1997, Fire Code under, O. Reg. 213/07 Retain as required by: CAN/CSA-C282-M89	FPPA-OR213s1.1.2.1 s. 1.1.2.1 O. Reg. 213/07, Division B, Part 6	Emergency Power Systems - Inspections/Testing	Permanent - Log of Operations Inspection and Testing, as required by CAN/CSA-C282-M89

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
FPPA-O-2	Fire Protection and Prevention Act, 1997, Fire Code under, O. Reg. 213/07	FPPA O.Reg 213 s. 2.8.3.3(3)	Fire Drill Records	E + 1 (event is the fire drill)
FPPA-O-3	Fire Protection and Prevention Act, 1997, Fire Code under, O. Reg. 213/07 See also National Fire Protection Agency Standard (NFPA) 10-2002	FPPA OR213s6.2.7.5 s. 6.2.7.5	Fire Extinguisher Maintenance/Testing (Portable)	Permanent - retain for life of equipment
FPPA-O-4	Fire Protection and Prevention Act, 1997, Fire Code under, O. Reg. 213/07	FPPA OR213s1.1.1.2 s. 1.1.1.2	Fire Protection Systems - Inspection and Testing	E + 2 (event is when the record was made) Note must ensure that the current and the immediately preceding report is available.
FPPA-O-5	Fire Protection and Prevention Act, 1997, Fire Code under, O. Reg. 213/07	FPPA O.R213s1.1.2.1 s. 1.1.2.1	Fire Protection Systems - Verification Report	E - Life of system for systems installed after November 21, 2007.
FPPA-O-6	Fire Protection and Prevention Act, 1997, Fire Code under, O. Reg. 213/07	FPPA O.R213s2.8.2.1(3) s. 2.8.2.1(3)	Fire Safety Plan	S (Keep until superseded). Note requires regular review not to exceed 12 months.

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
FPPA-O-7	Fire Protection and Prevention Act, 1997, Fire Code under, O. Reg. 213/07	FPPA O.R213s9.1.4.8 s. 9.1.4.8	Life Safety Study - Retrofit	Permanent - Retain on premises.
FPPA-O-8	Fire Protection and Prevention Act, 1997, Fire Code under, O. Reg. 213/07	FPPA OR213s1.1.1.2 s. 1.1.1.2	Storage Tanks - Above Ground and Underground	E + 2 (event is when the record was made) Note must ensure that current and the immediately preceding report is available.
ITA-C-1	Income Tax Act, R.S.C. 1985, c. 1 (5th Supp.) Income Tax Regulations under the, C.R.C. 1978, c. 945,	ITA-C R945s5800 s. 5800(1)(a) as am. SOR/82-879, s. 2	Corporate Books and Records Tax Requirements - Where Corporation Ceased	E + 2 (event is two years after the day that the corporation is dissolved). Note: General ledger, etc. must be kept for six years after corporation dissolved.
ITA-C-2	Income Tax Act, R.S.C. 1985, c. 1 (5th Supp.), Income Tax Regulations under the, C.R.C. 1978, c. 945,	ITA-CR945s5800(1) s. 5800(1) as am. SOR/82-879, s. 2	General Ledger and Transaction Summaries Where Business Ceased	C+ 6 Note: Retain general ledger and any special contracts or agreements necessary to an understanding of the entries in the general ledger or other book of final entry.

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
ITA-C-3	Income Tax Act, R.S.C. 1985, c. 1 (5th Supp.), See also Canada Revenue Agency, Income Taxation Circular 1c78-10R4 (Revised June 2005)	ITA-Cs230(1) s. 230(1) R.S., 1985, c. 1 (5th Supp.), s. 230; 1994, c. 21, s. 105; 1998, c. 19, s. 227	Tax Payment/Collection Records and Books	C + 6 Retain the books and every account and voucher necessary to verify the information.
ITA-O-1	Income Tax Act, R.S.O. 1990	ITA-Os39 s 39 as am. S.O. 1999, c. 9, s. 129	Income Tax Accounting Records	C + 6
ITA-O-2	Income Tax Act, R.S.O. 1990,	ITA-Os48 cs. 48(3) R.S.O. 1990, c. I.2, s. 48 (3); 2004, c. 16, s. 3	Income Tax Offences - Limitation	Limitation - eight years.
ISA-O-1	Insurance Act, R.S.O. 1990,	IA-O s259.1 s. 259.1 2002, c. 24, Sch. B, s. 39 (3).	Automobile Insurance - Limitation	Limitation period - one year.
ISA-O-2	Insurance Act, R.S.O. 1990,	IA-Os148(1)14 148(1) 14 R.S.O. 1990, c. I.8, s. 148.	Fire Insurance Claims - Limitation	Limitation - one year after the loss or damage.
LTTA-O-1	Land Transfer Tax Act, R.S.O. 1990, c. L.6	LTTA-Os9.3(4)	Taxation Documents	E + 7 (event is date on which the conveyance registered)

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
LA-O-1	Limitations Act, 2002, S.O. 2002, c. 24, Sch. B	LA-Os4 s. 4 2002, c. 24, Sch. B, s. 4	Basic Limitation Period	E + 2 (event is act or omission on which the claim is based took place)
LA-O-2	Limitations Act, 2002, S.O. 2002, c. 24, Sch. B,	LA-Os15 s. 15 2002, c. 24, Sch. B, s. 15(1)	Ultimate Limitation Period	E + 15 (event is act or omission on which claim is based took place)
MFIPPA-O-1	Municipal Freedom of Information and Protection of Privacy Act General Regulation under the, R.R.O. 1990, Reg. 823	MFIPPA-OR823s5 s. 5 R.R.O. 1990, Reg. 823, s. 5	Personal Information Retained by Institutions	E + 1 (event is the date or time that the information was used) Note: This is a minimum retention period only. Personal information may be retained longer for a legal or operational need, providing notification is given.
OHSA-O-1	Occupational Health and Safety Act - R.R.O. 1990 Designated Substance - Asbestos on Construction Projects and in Buildings and Repair Operations Regulation 278/05	OHSA-Os8 s. 8 O. Reg. 278/05, s. 8(1)	Asbestos Management in Buildings	Not specified - Retain on premises.
OHSA-O-2	Occupational Health and Safety Act - R.R.O. 1990	OHSA-Os9(22) s. 9(22) R.S.O. 1990, c. O.1, s. 9(1)	Joint Health and Safety Committee Minutes	Not specified.

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
OHSA-O-3	Occupational Health and Safety Act - R.R.O. 1990	OHSA-Os12(2) s. 12(2) R.S.O. 1990, c. O.1, s. 12 (1); 1997, c. 16, s. 2(4)	Workers' Compensation Board Annual Summary	Not specified. Post copy of summary.
OHSA-O-4	Occupational Health and Safety Act - R.R.O. 1990	OHSA-Os26(1) s. 26(1) R.S.O. 1990, c. O.1, s. 26 (3); 1994, c. 27, s. 120(3)	Biological/Chemical/Physical Agents Handling/Exposure Records	Keep and maintain accurate records of the handling, storage, use, and disposal of biological, chemical, or physical agents as prescribed by regulation and make available to workers (see specific regulation).
OHSA-O-5	Occupational Health and Safety Act - R.R.O. 1990 c. O.1, s. 37(5) and s. 38; as am. S.O. 2001, c. 9, Sch. I, s. 3(8)	OHSA-Os38 s. 38 2001, c. 9, Sch. I, s. 3(8)	Material Safety Data Sheets	E + 3 (event is creation or modification of the data sheet)
OHSA-O-6	Occupational Health and Safety Act - R.R.O. 1990 Designated Substance - Asbestos on Construction Projects and in Buildings and Repair Operations Regulation 278/05	OHSA-OR278s18(9) s. 18(9) O. Reg. 278/05, s. 18(9)	Airborne Asbestos Monitoring Records - Type 3	E + 1 (event is the date results are received)
OHSA-O-7	Occupational Health and Safety Act - R.R.O. 1990 Confined Spaces, Regulation 632/05	OHSA-OR632s21 s. 21 O. Reg. 632/05, s. 21(1)	Confined Spaces Records - Plan/Assessments/Training/ Permits/Inspection of Rescue Equipment/Testing Results	E + 1 Note - must ensure that the two most recent reports are retained.

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
OHSA-O-8	Occupational Health and Safety Act - R.R.O. 1990 Designated Substance - Isocyanates Regulation, under the R.R.O. 1990, Reg. 842,	OHSA-OR842s13 s. 13 R.R.O. 1990, Reg. 842, s. 13	Airborne Isocyanates Monitoring and Exposure Records	E + 5 (Exposure records to be forwarded to physician for retention for E+40 date of first record and E+20 date of last record)
OHSA-O-9	Occupational Health and Safety Act - R.R.O. 1990 Designated Substance - Lead Regulation, under the R.R.O. 1990, Reg. 843	OHSA-OR843s12 s. 12 R.R.O. 1990, Reg. 843, s. 12	Airborne Lead Monitoring and Exposure Records	E + 5 (Exposure records to be forwarded to Physician for retention for E+40 date of first record and E+20 date of last record)
OHSA-O-10	Occupational Health and Safety Act - R.R.O. 1990 Designated Substance - Mercury Regulation, under the R.R.O. 1990, Reg. 844	OHSA-OR844s12 s. 12 R.R.O. 1990, Reg. 844, s. 12	Airborne Mercury Monitoring and Exposure Records	E + 5 (Exposure records to be forwarded to Physician for retention for E+40 date of first record and E+20 date of last record)
OHSA-O-11	Occupational Health and Safety Act - R.R.O. 1990 Designated Substance - Silica Regulation, under the R.R.O. 1990, Reg. 845,	OHSA-OR845s12 s. 12 R.R.O. 1990, Reg. 845, s. 12	Airborne Silica Monitoring and Exposure Records	E + 5 (Exposure records to be forwarded to Physician for retention for E+40 date of first record and E+20 date of last record)
PBA-O-1	Pension Benefits Act, R.S.O. 1990,	PBA-Os110 s. 110(6) as am. S.O. 1997, c. 28, s. 220(2)	Pension Benefits - Limitation	Limitation - five years after the date when the offence occurred.

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
PHIPPA-O-1	Personal Health Information and Protection Act The College of Psychologists of Ontario, The Regulations, Standards of Professional Conduct and Guidelines of the College of Psychologists of Ontario, revised version effective September 1, 2005.	CPO - Standards	Psychological Service Records	E + 10 (event is 10 years from date of last contact, or 10 years following the client's 18th birthday)
RPLA-O-1	Real Property Limitations Act R.S.O. 1990, C. L.15	RPL-Os22 s. 22 R.S.O. 1990, c. L.15, s. 22	Mortgages Arrears - Limitation	Limitation - 10 years after the last payment of any part of the principal money or interest secured by the mortgage
RPLA-O-2	Real Property Limitations Act R.S.O. 1990, C. L.15	RPLA - Os4 s. 4 R.S.O. 1990, c. L.15, s. 4	Recovery of Land - Limitation	Limitation - 10 years from the right to make or bring action first occurred
RPLA-O-3	Real Property Limitations Act R.S.O. 1990, C. L.15	RPL-Os17 s. 17(1) R.S.O. 1990, c. L.15, s. 17(1)	Rent Arrears - Limitation	Limitation - Six years next after the same respectively has become due
SDWA-O-1	Safe Drinking Water Act, 2002, S.O 2002, C. 32, Schools, Private Schools and Day Nurseries, O Reg. 243/07	SDWA-0R243s9(1) s. 9(1) O. Reg. 243/07, s. 9(1)	Drinking Water - Flushing Tests	C + 6

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
C + 6	TSSA-O-1 Technical Standards and Safety Act, 2000, Elevating Devices Regulation, under the 2000, O. Reg. 209/01	TSA-OR209s38 s. 38 O. Reg. 209/01, s. 38	Elevator Contractor and Equipment Contacts	Not specified - Maintain for life of equipment/building. Retain: • name and telephone number of the contractor currently maintaining the elevator, and expiry date of contract • location of keys to be posted inside the firehose cabinet
TSSA-O-2	Technical Standards and Safety Act, 2000, Elevating Devices Regulation, under the 2000, O. Reg. 209/01	TSA-Or209s37 s. 37 O. Reg. 209/01, s. 37	Elevator Design Submissions/Instructions	Not specified. Retain: • list of people to be called in case of power failure or accident at the location of the installation • a copy of the registered design submissions for • general instructions for maintenance.
TSSA-O-3	Technical Standards and Safety Act, 2000, Elevating Devices Regulation, 2000, O. Reg. 209/01	TSA-OR209s34 s. 34 O. Reg. 209/01, s. 34(1)	Elevator Equipment Contacts	Not specified. Retain: • a list of persons to be called in case of an equipment or power failure, an accident, or any other emergency involving the elevating device, to be made is readily available at the location of the installation • ensure that the person called is prepared to take such action as is appropriate in the circumstances
TSSA-O-4	Technical Standards and Safety Act, 2000, Elevating Devices Regulation, under the 2000, O. Reg. 209/01,	TSA-OR209s30 s. 30 O. Reg. 209/01, s. 30(1)	Elevator License	Not specified - Post for life of equipment.

Reference Code	Governing Statute (Linked to e-laws or CanLII)	Citation Alpha Code (Linked to governing statute or regulation if applicable)	Title Words/Key Words	Retention Requirement or Limitation Period
TSSA-O-5	Technical Standards and Safety Act, 2000, Elevating Devices Regulation, under the 2000, O. Reg. 209/01	TSA-OR209s34 s. 34 O. Reg. 209/01, s. 34(1) O. Reg. 209/01, s. 34(2) O. Reg. 209/01, s. 34(3)	Elevator Log Book	E + 5 (event is the date of the last entry in the log book)
TSSA-O-6	Technical Standards and Safety Act, 2000, Elevating Devices Regulation, under the, 2000, O. Reg. 209/01,	TSAS33s33 s. 33(6) O. Reg. 209/01, s. 33(6)	Elevator Maintenance Records	E + 5 (event is date of last entry in the log book.) *Maintain in log book.
WSIA-O-1	Workplace Safety and Insurance Act, 1997, S.O. 1997, c. 16, Sch. A	WSIA-Os157 s. 157 as am. S.O. 1995, c. 5, s. 27	Workers' Compensation Restriction on Prosecution	E + 2 (event is two years after the day on which the most recent act or omission comes to the knowledge of the board)
WSIA-O-2	Workplace Safety and Insurance Act, 1997, S.O. 1997, c. 16, Sch. A First Aid Requirements, Regulation 1101	WSIA-OR1101s5 s. 5 R.R.O. 1990, Reg. 1101, s. 5	Accident Report and Record of Administration of First Aid	No retention period specified.

Purpose

The model classification and retention scheme is a provided as a sample scheme for school boards/authorities to consider developing their own records and information management program. School boards/authorities will need to adapt and adjust this model to reflect their local needs and practices. This includes establishing an internal review and approval process for recommended retention periods so that the recommended retention satisfies board operational and litigation needs. The goal is to develop an organization-wide strategy that reflects statutory requirements and current practices and considers the management of both paper and electronic records and information.

The model includes recommended retention periods which reflect the retention periods specified in laws of Canada and Ontario (see Tables of Statutes and Citations of Laws of Canada and Ontario-based Records Retention Requirements). It should be used in concert with the PIM Taskforce Guideline on the Model Classification Scheme and Retention Schedule. Where retention periods are not specified in law, the recommended retention is based on operational need and recommended best practices in records management.

It is also important to understand that schemes and schedules are “living” or “evergreen” documents and can not be considered “complete” at any point. Updates and revisions to both the nature of records retained and the retention periods applied to them continuously evolve. Boards/authorities need to ensure that their programs are routinely reviewed and revised to accommodate these updates. For this reason, and to provide for feedback from various school boards/authorities, this document is being released as a draft. A more final scheme will be released with the DVD and as part of the regional training sessions.

P – Permanent Retention	E – Event (retention begins once an event or action occurs, e.g., the creation of the record, retirement of a student)	C – Current (retain for the current school or fiscal year)	S – Superseded (retain until a new version replaces the current one) Note: S + 1 = Retain both current and previous version

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
ADM	Administrative Management	The function of overseeing the administration of the team and units within the board/authority and schools. Records supporting this function relate to administrative committees' decisions and meetings, and internal administrative support or services. The functions of acquiring and managing equipment, supplies, services and materials for schools.											

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
ADM	Associations/ Organizations	Includes reports, newsletters, publications, conference and workshop information and proceedings from organizations to which staff belong.	Originating Department	C + 1	1	C + 2	C + 1						Operational value
ADM	Meeting Documentation: External	Includes records of external committees and councils on which board and school staff members participate as members. Records include agendas, reports, resolutions and any documentation which reflects obligations of the board.	Originating Department	E + 1	1	E + 2	E					E = the date the board became a member of the committee.	Operational value
ADM	Meeting Documentation: Internal	Includes records regarding staff meetings, student council and committees such as principals' council, secretaries' meetings, as well as district and subject head meetings. Records include agendas, minutes, reports and resolutions. Excludes governance	Originating Department	C + 1	3	C + 4	C + 1			Archival Review			Operational value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		committees (e.g., admin. council, exec. council, etc.).											
ADM	Forms Inventory	Includes forms history and blank copies of forms, kept on file for convenience.	Originating Department	S + 1		S + 1	S			Archival Review			Operational value
ADM	Requests for Information	Includes requests and tracking sheets for Freedom of Information Requests made under the *Municipal Freedom of Information Act* and requests for access to student/employee records and information.	FOI School HR	E + 2	-	E + 2	E + 1		PIB			E= final resolution of request (or appeal if applicable).	MFIPPA-O Operation value
ADM	Library Management	Includes records related to board/school library operations. Records include collection inventories, correspondence, acquisition and disposal planning and strategies, and other records related to library holdings and operations.	Library Services	S + 1	-	S + 1	S + 1		PIB			S = when inventories are updated and library weeding out is done.	MFIPPA-O Operational value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
ADM	Service Requisitions and Reports: Internal Services	Includes records relating to translation, audio visual services, duplicating/ printing services and mail/courier and delivery services. Records include requisitions and memos for services, confirmations and service logs/reports, correspondence, reports, etc.	Originating Department	C + 1	-	C + 1	C + 1						Operational value
ADM	Records Destruction Notices	Documentation relating to which records have been destroyed in the normal course of business. Includes lists of destroyed records and forms authorizing the destruction of records.	Records Management	P	-	P	P	Vital				Evidence of application of records program to support litigation if required.	Legal value
ADM	Records Management Listings	Includes information regarding the management of records,	Records Managemen	S + 1	-	S + 1	S + 1	Vital				S = when new reports are	Legal value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
	and Reports	regardless of medium. Records include Classification Scheme, Legal Citation Table, file lists, lists of records in storage, records management reports and related correspondence.	t									received	
ADM	Vendors/ Suppliers/ Contractors	Includes information about vendors, contractors and suppliers and their goods and services. Records include catalogues, price lists and correspondence. Excludes agreements and purchasing documentation, etc.	Originating Department	S	-	S + 1	S					S = when new documentation is received from suppliers.	Operational value
COM	Communications and Public Relations	The function of promoting and marketing boards/authorities/schools and programs and services. Records in this function include board/authority/school communication and press releases, speeches, websites, public relations											

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		activities, events and news releases; materials relating to marketing research, publications and reports.											
COM	Advertisements	Includes publications, artwork and copies of advertisements placed by the board or schools. Excludes website records.	Originating Department	C + 1	3	C + 4	C			Archival Review			Operational value
COM	Appreciation and Commendations	Includes general commendations, certificates of appreciation and petitions received from the general public and parents. Excludes: records relating to specific employees or student records.	Originating Department	C + 1	-	C + 1	C						Operational value
COM	Communiqués	Includes memos, brochures, correspondence and related information about programs and activities sponsored by the board or by schools.	Originating Department	C + 1	3	C + 4	C			Archival Review			Operational value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
COM	Complaints	Includes records related to general complaints about the board/authority/ school and its activities. Includes correspondence, investigations, findings and related reports regarding resolution. Complaints about a specific project or program may be contained within the program. Excludes complaints specific to an individual student or staff member – see case files.	Originating Department	E + 1		E + 1	E		PIB			E = resolution of complaint.	MFIPPA-O
COM	Contacts and Mailing Lists	Includes lists of individuals or organizations with whom the board/authority and school communicate. Records include mailing lists, emergency contact lists, student lists, etc.	Originating Department	S	-	S	S		PIB			S = when lists are updated.	MFIPPA-O Operational value
COM	Events, Ceremonies and Celebrations	Includes memos, notices, correspondence with parents and others, programs and all related materials pertinent to events sponsored by the	Originating Department	C + 1	3	C + 4	C			Archival Review			Operational value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		board or by schools (e.g., parents' night, school opening ceremonies, reunions, etc.). Records include program schedules, correspondence, brochures, and event activity details.											
COM	Media Kits, Communications and News Releases	Includes records regarding board relations with the various media. Includes press releases and information releases, speeches, photographs, correspondence, etc.	Originating Department	C + 1	3	C + 4	C + 1			Archival Review			Operational value
COM	Memorabilia	Includes school/board memorabilia, collectibles and other historical items that reflect the individual nature of the schools, such as informal school/board/ authority histories, school logos and crests, songs, etc.	Originating Department	C + 1	3	C + 4	C + 1			Archival Review		These publications may have historical value. If the school/board/ authority does not maintain a historical collection, consideration should be given to changing the retention	EA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
												period to permanent.	
COM	Multimedia Materials	Includes photographs, slides, videotapes, CDs, DVDs, recordings, etc. that document school and board activities.	Originating Department	S + 1		S + 1	S + 1			Archival Review		These publications may have historical value. If the school/board/ authority does not maintain a historical collection, consideration should be given to changing the retention period to permanent.	EA-O
COM	News Reports	Includes news reports from newspapers, magazines, websites and other publications regarding the board/ authority, school, staff, students and trustees. May be paper or electronic.	Originating Department	C + 3	-	C + 3	C			Archival Review			EA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
COM	Publications: Internal	Includes records and artwork for publications such as yearbooks, curriculum handbooks, school handbooks, school calendars, "Welcome to High School" booklets, annual reports, brochures on programs offered by schools, newsletters, and other school promotions.	School/ Originating Department	S + 1	3	S + 5	S		PIB	Archival Review		These publications may have historical value. If the school/board/ authority does not maintain a historical collection, consideration should be given to changing the retention period to permanent.	EA-O MFIPPA-O
COM	Speeches and Presentations	Includes speeches and presentations delivered by board/authority/school staff, elected officials and teachers covering non-classroom topics.	Originating Department	C + 4		C + 4	C + 1			Archival Review		These publications have historical value. If the school/board/authority does not maintain a historical collection, consideration should be given to changing the retention period to permanent.	EA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
COM	Website content	Includes snapshots of website content and copies of web pages created by school boards for general public use. Includes board/authority and school sites.	Originating Department	C + 1	3	C + 4	C + 1			Archival Review		These publications have historical value. If the school/board/authority does not maintain a historical collection, consideration should be given to changing the retention period to permanent.	EA-O Operational value Legal Value
FAC	Facilities Management	The function of managing and maintaining board/ authority buildings and facilities and supporting capital initiatives and building improvements. Records include maintenance and operations reports, requests and logs, environmental testing of facilities, equipment maintenance and testing, facilities planning and improvements, capital and											

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		non-capital projects, inspection reports, and records relating to property acquisition and disposition, building and office renovations, security, and property management relationships.											
FAC	Building and Site Approvals	Includes documentation such as site plan approvals, building permits, Life Safety Plan and municipal reports pertaining to the approval of building plans by the municipality, Fire Marshal's Office, Ministry of Education, Ministry of Health, and other government bodies.	Facilities	E + 1	5	E + 6	E					E = as long as building remains board property.	BCA-O FPPA-O TSSA-O Operational value Legal Value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
FAC	Inspection and Testing Logs and Reports: General	Includes all documentation to support the inspection and testing of buildings, equipment, physical plant and property. Records include logs, inspection reports, year-end reports, equipment lists and locations. Includes water flushing logs, water testing reports, elevator logs, sanding and salting logs, playground equipment inspections logs, chemical treatment log, underground storage tank inspections, playground inspections, physical education equipment inspections, technical program equipment, etc. Excludes contractor logs, air quality testing, Health and Safety inspection reports, emergency power systems inspections and	Facilities/ Custodian (as designated by the board)	E + 1	5	E + 6	E					E = date the record was created Note: Must ensure that at least current and immediately preceding reports are retained.	FPPA-O SDWA-O TSSA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		testing, fire extinguisher testing, fire protection systems testing.											
FAC	Inspections Logs and Reports: Fire Protection Systems and Emergency Power Systems	Includes records regarding the inspection and testing of emergency power systems, fire extinguishers and fire protection systems.	Facilities	E + 1	1	E + 2	E					E = life of equipment.	FPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
FAC	Facilities Construction Projects	Includes budgets, estimates, project plans and schedules, progress reports, project meeting minutes, certificates of clearance, project drawings and correspondence regarding the building of schools and other properties. Excludes capital projects financing and financial records related to construction dispersements.	Facilities	E + 1	5	E + 6	E						BCA-O FPPA-O TSSA-O
FAC	Facilities Improvement Projects	Includes project records regarding the building improvements program and supporting documents specific to additions, renovations, and alterations to schools and buildings. Records include drawings, project plans, specifications, meeting minutes, project updates, budgets, etc.	Facilities	E + 1	5	E + 6	E					E = completion of project (superficial improvements). **Upon project completion, certain records may be transferred to building maintenance and operations files for**	BCA-O ITA-C ITA-O ETA-C FPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
												ongoing operational support.	RPLA-O
FAC	Drawings and Specifications	Includes technical specifications for a project or property, e.g., mechanical, electrical and structural. Includes building and fire code requirements and architect's instructions. Includes all drawings and plans of schools and offices, such as master drawings and floor plans, site plans, aerial plans, and plans for additions and	Facilities	E	15	E + 15	E	Vital		Archival Review		E = as long as building remains board property.	RPLA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		alterations.											
FAC	Emergency Plans	Includes records regarding emergencies and related plans to support the board/authority/school in case of fire or other emergencies. Records include emergency plans, business continuity plans, call lists, supplier/vendor contacts, and related reports.	School/ Facilities	S + 1	4	S + 5	S	Vital		Archival Review			Operational value
FAC	Designated Substances and Hazardous Materials – Waste Monitoring and Management	Includes records related to the management and disposal of chemical, biological or physical agents or substances.	Facilities/ Health and Safety	C + 1	2	C + 3	C						OHSA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
FAC	Designated Substances and Hazardous Material Monitoring : Hazardous Biological, Chemical or Physical Agents	Includes records regarding the monitoring of hazardous chemical and physical agents and designated substances in accordance with the *Occupational Health and Safety Act.* Includes air quality reports. Excludes exposure records of workers.	Facilities	E + 1	4	E + 5	1					E = when the record was first created.	OHSA-O
FAC	Confined Spaces	Includes records relating to the assessment of confined spaces and written plan and procedures for the control of hazards in confined spaces. Excludes training records. See **HUM**.	Facilities	E +1		E + 1						E = when the record was first created. Note: Must ensure that the two most recent reports are retained.	OHSA-O

MODEL CLASSIFICATION AND RETENTION SCHEME FOR SCHOOL BOARDS/AUTHORITIES

PIMtoolkit

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
FAC	Facilities Planning	Includes records regarding the allocation of classroom and workspace to staff and students. Records include correspondence, proposed enrolment studies and reports, facilities use plans, facilities designs and layouts, furniture layouts, etc.	Facilities	C + 1	3	C + 4	C + 1						Operational value
FAC	Health and Safety Committee	Records include reports, correspondence, minutes of health and safety committee meetings, notices, correspondence and reports	Facilities	C + 1	2	C + 3	C + 1						OHSA-O
FAC	Incident Reports: Health and Safety and Student Safety	Includes general records relating to incidents that affect health and safety of staff and/or students, e.g., emergency response, school illness, infections, quarantines, etc. Records include reports, correspondence and summaries and information related to	Facilities	E + 1	5	E + 6	E					E = resolution of issue. Note: Depending on the nature of the incident, records may have legal value.	OHSA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		actions taken by staff. Excludes employee medical health records (personally identifiable records).											
FAC	Health and Safety Inspection Reports	Includes records of inspections carried out by the Health and Safety Committee in accordance with the *Occupational Health and Safety Act.*	Health and Safety	C + 1	1	C+1	C + 1					Note: A minimum of two inspection reports must be retained.	OHSA-O
FAC	Land Surveys	Includes land survey information such as legal property surveys, construction layout and control surveys, and field notes. Also includes soil-boring reports.	Facilities	S	-	S	S			Archival Review		Ensure that land surveys are available at local registry office before destruction.	
FAC	Maintenance and Operations: Buildings/ Physical Plant and Equipment	Includes records related to support the maintenance and operations of buildings, physical plant and equipment. Includes office equipment.	Facilities	E+ 1	2	E + 3	E + 1					E = disposal of facility or equipment.	FPPA-O TSSA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
FAC	Maintenance and Operations: Grounds	Maintenance requisitions, work orders, logs and reports showing action taken re grounds keeping, snow clearance, and cleaning.	Facilities	C + 1	1	C + 2	C						Operational requirement
FAC	Material Safety Data Sheets	Includes material safety data sheets as created and issued by the manufacturer.	Facilities	E + 3	-	E + 3	E + 3					E = creation or revision of the MSDS. Note: Every location that uses the material must retain a copy of the data sheet.	OHSA-O
FAC	Permits/ Facility Bookings	Includes copies of permits issued by the board/ authority for the use of school property for purposes such as polling stations and community events. Also includes applications for permits, lists of permit holders and inter-jurisdictional permits.	Originating Department	C + 1	3	C + 4	2						Operational value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
FAC	Security	Includes records regarding the security of office and school facilities and properties such as control of keys, trespassing, surveillance reports, emergency telephone numbers/contacts, and police station locations. Also includes school visitor book and contractor logs, etc.	Facilities	S + 2	-	S + 2	2		PIB				EA-O MFIPPA-O
FAC	Vehicles/Fleet Management	Includes records of all vehicles currently owned, operated and maintained by the board.	Facilities	E + 2	-	E + 2	E					E = disposal of vehicle.	CAI-O LA-O
FIN	Finance and Accounting	The function of managing board/authority/school financial and accounting resources. Includes establishing and operating and maintaining accounting (payables, receivables, revenue) systems, controls and procedures, financial planning, reporting,											

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		preparing budgets and budget submissions, and the monitoring and analysis of capital assets. Records include but are not limited to accounts payable and receivable, budgets, audits, benefits accounting, expense payments, financial reporting, fixed asset management and all matters regarding the allocation and control of funds.											
FIN	Accounts Payable	Includes records documenting funds payable such as legal fees, trustees and employees expenses, vendor transaction listings, payment vouchers, cheque requisitions, gas, hydro and phone bills, petty cash disbursements. PIB for staff and board expense.	Finance	C + 1	5	C + 6	C + 1		PIB				ETA-C ITA-C ITA-O ECA-0 MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
FIN	Accounts Receivable	Records related to the accounting for money owed to schools and boards. Records include invoices, cash receipts, correspondence, cash lists and statements of account	Finance	C + 1	5	C + 6	C + 1	Vital					ETA-C ITA-C ITA-O ECA-0
FIN	Audits - Financial	Includes records regarding internal and external financial audits of accounts.	Finance	C + 1	5	C + 6	C + 1	Vital					ETA-C ITA-C ITA-O ECA-0
FIN	Banking and Cash Management	Includes records regarding banking transactions and relationships with banks. Includes bank statements, bank reconciliations, deposit records, cancelled cheques, cheque stubs and money order rates.	Finance	C + 1	5	C + 6	C + 1	Vital					ETA-C ITA-C ITA-O ECA-0

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
FIN	Budgets	Includes departmental and board budgets, both capital and operating. Includes all working notes, budget formula calculations, current estimate highlights, preliminary formula budget calculation sheet summaries, and budgeted vs. actual reports.	Finance	C + 1	5	C + 6	C + 1						ETA-C ITA-C ITA-O ECA-0
FIN	Capital Projects: Financing	Includes records relating to the financing of capital projects. Includes quarterly reports, working papers, building monthly costs, capital payment vouchers, approvals, costing, capital expenditure forecasts and correspondence with architects and contractors.	Finance	E + 1	5	E + 6	E + 1					E = completion of project.	ETA-C ITA-C ITA-O ECA-0
FIN	Capital Revenue	Includes records related to capital revenue from sale of property and rental income from leased premises and other sources.	Finance	C + 1	5	C + 6	C + 1		Vital				ETA-C ITA-C

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
													ITA-O ECA-0
FIN	Cost Allocations	Includes records relating to allocation of tuition and other costs between school boards/authorities. Records include correspondence, reports and related supporting documentation.	Finance	C + 1	5	C + 6	C + 1		Vital				ETA-C ITA-C ITA-O ECA-0
FIN	Financial Forecasts and Reports	Includes records relating to general ledger balancing, including GL reports, variance reports, yearly schedule, variance report changes.	Finance	C + 1	5	C + 6	C + 1						ETA-C ITA-C ITA-O ECA-0
FIN	Financial Statements	Includes the balance sheet, income statement, statement of source and application of funds, and other audited financial	Finance	C + 1	Life of Board/ Authority	Life of Board /	C + 1		Vital				ETA-C ITA-C

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		statements.				Authority							ITA-O ECA-0
FIN	Financial Work Papers	Includes all drafts, grant calculations and other working papers associated with the development of financial statements.	Finance	C + 1	5	C + 6	C + 1						ETA-C ITA-C ITA-O ECA-0
FIN	Funding – External Sources	Records relate to bequests and donations, grants and subsidies (including government), and ISA claims. Records include correspondence, background information and supporting documentation.	Finance	E + 1	5	E + 6	E + 1	Vital				E = winding up of fund/bequest or expiry of grant period.	ETA-C ITA-C ITA-O ECA-0

MODEL CLASSIFICATION AND RETENTION SCHEME FOR SCHOOL BOARDS/AUTHORITIES

PIMtoolkit

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
FIN	Funding Assessments	Includes records relating to the direction of school support, levies and related assessments. Also includes information on fee-paying, non-resident and international visa students.	Finance	C + 1	5	C + 6	C + 1						ETA-C ITA-C ITA-O ECA-0
FIN	Funding: Student Council	Includes records on funds allocated to or raised by the student council. Records consist of accounts receivable and payable documents such as invoices and vouchers.	Finance	C + 1	5	C + 6	C + 1	Vital					ETA-C ITA-C ITA-O ECA-0
FIN	Fundraising: Charitable Organizations	Includes records regarding the raising of funds for charitable organizations. Records include completed contribution forms, promotional materials for fundraising and reports	Originating Department	C + 1	5	C + 6	C + 1	Vital					ETA-C ITA-C ITA-O ECA-0

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
FIN	Inventory Control: Fixed Assets	Records relating to the balance sheet, including fixed asset listings, depreciation details, asset transfer information, and details of extraordinary entries.	Finance	E + 1	P	P	E + 1	Vital				E = disposal of asset.	ETA-C ITA-C ITA-O ECA-0
FIN	Inventory Control: Non-fixed assets	Includes all records regarding inventories of board-/authority-owned equipment. Excludes hazardous materials inventories	Finance	C + 1	5	C + 6	C + 1						ETA-C ITA-C ITA-O ECA-0
FIN	Investments	Includes records regarding the board's investments, term deposits and promissory notes. May also include records of investments in fuel for later sale to individual schools and other	Finance	E + 1	5	E + 6	E + 1	Vital				E = after closure of account, redemption of issue.	ETA-C ITA-C ITA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		organizations involved in the bulk purchase. Includes records regarding the debentures and bonds issued. Includes information on the initial issuance of the debenture or bond and records of payments made to investors.											ECA-0
FIN	Journal Vouchers and Journal Entries	Includes completed journal voucher forms, input forms, and all background documentation used to substantiate journal entries.	Finance	C + 1	5	C + 6	C + 1						ETA-C ITA-C ITA-O ECA-0
FIN	Ledgers: General	Includes all records in the books of original entry, whether maintained in book format or as a computer report.	Finance	C + 1	Life of School/ Board/ Authority	Life of School / Board / Autho	C	Vital				General ledgers of discontinued or dissolved school boards should be sent to the Ministry of Education.	ETA-C ITA-C ITA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
						rity							ECA-0
FIN	Ledgers: Subsidiary Ledgers, Registers and Journals	Includes all subsidiary ledgers, registers and journals such as payment and receipt journals, payroll registers, purchase order registers, and year-end adjustments.	Finance	C + 1	5	C + 6	C + 1						ETA-C ITA-C ITA-O ECA-0 LA-O RPLA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
FIN	ONSIS Reporting:	Includes all counts and projections documenting enrolments in the school system and statistical reports required by the Ministry of Education as part of the funding process for the preparation of educational statistics, e.g.,October and March school/board/authority reports.	Finance	C + 1	5	C + 6	C + 1			Archival Review		2008 discussions with the Ministry OnSIS group indicate that there is no specified retention period for these reports. The current retention period is based on the need to support other financial data.	
FIN	Payroll Management	Includes all records of payments of salary, wages and deductions to employees. Includes payroll master cards, time sheets, direct deposit request forms, payroll update logs, holdbacks, and payroll deduction and billing reports. Also includes T4's, TD's, and ROE's.	Finance	C + 1	C + 5	C + 6	C + 1	Vital					ETA-C ITA-C ITA-O ECA-0

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
FIN	Pension Contributions/ Support	Includes contribution cards detailing pension and benefits obligations due to retired employees under OMERS and other annuity or superannuation plans (TPP). Includes payroll records required to determine and verify pension payments.	Finance	E + 1	E + 5	E + 6	E + 1	Vital				E = until pension is paid out to all beneficiaries.	ETA-C ITA-C ITA-O ECA-0
FIN	Purchasing Documentation	Records supporting purchases made by the school/board/authority. Includes purchase requisitions, purchase orders, requests for proposal, requests for quotations, specifications, invitations to tender, proposals, tender submissions, bid and performance bonds, and all documentation regarding the selection process.	Finance	C + 1	C + 5	C + 6	C + 1	Vital					ETA-C ITA-C ITA-O ECA-0

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
FIN	Income Tax Returns	Records relating to federal and provincial income tax returns, including signed income tax returns and supporting documents submitted to federal and provincial tax agencies.	Finance	C + 3	Life of Board/ Authority	Life of Board / Authority	C + 1						ETA-C ITA-C ITA-O ECA-0
FIN	Sales and Property Tax Returns and Reports	Includes records documenting taxation such as gas surtax reports, income tax returns, and federal sales tax tables. Also includes Goods and Services Tax returns and requests for rebate.	Finance	C + 1	5	C + 6	C + 1						ETA-C ITA-C ITA-O ECA-0
FIN	Transportation Reports and Costing	Includes records on bus route costing, fuel rates, bus capacity loading, and records regarding the escalation and de-escalation of fuel prices for vehicles and buses and its impact on the Bus Transportation Contract	Originating Department	C + 1	5	C + 6	C + 1						ETA-C ITA-C ITA-O ECA-0

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		with the Bus Line Operators.											
GOV	Governance	The function of governing boards/authorities/schools and exercising legal authority and control. The corporate governance structure specifies the distribution of rights and responsibilities among different participants in boards/authorities/ schools, such as the board and staff, and spells out the rules and procedures for making decisions on it affairs. Includes resolutions, bylaws, policies and procedures, charters, board meeting administration, and strategic planning.											

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
GOV	Appointments: Board and Committee Members	Includes records on recommendations made by the board regarding appointments to other local boards such as the library board, board solicitors, banking authority and auditor.	Board Secretary	E + 1	-	E + 1	E + 1			Archival Review		E = expiry of term of office.	EA-O
GOV	Articles of Incorporation, By-laws and Constitution	Includes records related to the operation of the school board and capture details about the legal entity.	Board Secretary	S + 1	Life of Board/ Authority	Life of Board / Authority	S			Archival Review		S = changes made to documentation.	EA-O
GOV	Audits - Program	Includes audits of programs, curriculum plans and related board/ authority and school activities undertaken by the Ministry of Education.	Originating Department	E + 1	5	E + 6							EA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
GOV	Meetings: Board of Directors	Includes agenda and related reports meetings, working notes used in agenda preparation, minutes, resolutions and meeting briefs	Board Secretary	C + 5	Life of Board/ Authority	Life of Board / Authority	C + 1			Archival Review			EA-O
GOV	Meetings: Governance Committees and Councils	Includes agenda and minutes of school standing, advisory and ad hoc committees. May include school council, administrative council, directors' council; steering, standing, and advisory committees; task forces; the Employee Assistance Program advisory committee; and Special Education advisory committee.	Board Secretary	C + 5	Life of Board/ Authority	Life of Board / Authority	C + 1			Archival Review			EA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
GOV	Guidelines, Policies and Directives: External	Includes documentation about initiatives and guidelines provided by the Ministry of Education. Records include memoranda, directives, and correspondence such as the OSR Guideline, EIC Guidelines and Ministry Policy/Program Memoranda.	Board Secretary	S + 3	-	S + 3	S					S = when policies and directives are replaced. Board/authority/school can obtain old copies from Ministry if required.	EA-O
GOV	Guidelines, Policies and Directives: Internal	Includes records relating to board and school operating practices and activities. policy and procedure manuals, guidelines and directives, and all other policies and procedures established by the board, departments and schools, such as accounting procedures, emergency procedures, evaluation procedures, records management, personnel, and attendance reporting procedures.	Originating Department	S + 1	Life of Board/ Authority	Life of Board / Authority	S			Archival Review		S = when policies and procedures are replaced. Core records to show evolution of school/board/ authority.	EA-O FPPA-O OHSA-O

MODEL CLASSIFICATION AND RETENTION SCHEME FOR SCHOOL BOARDS/AUTHORITIES

PIMtoolkit

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
GOV	Intergovernmental Reporting and Communication	Includes correspondence and reports between the board and various levels of government such as the municipality, provincial ministries, etc. Also includes correspondence and information on other school boards.	Originating Department	C + 1	5	C + 6	C + 1			Archival Review			EA-O
GOV	Organization Structure	Includes records regarding reporting relationships, organization structure, organization analysis, etc. For both schools and school boards/authorities. Includes organizational charts and school profiles.	Originating Department	S + 1	-	S + 1	S			Archival Review		S = when organization structure changes.	EA-O
GOV	Trustee Management	Includes clerk's certificate, elections information, personal information, directories and news items regarding the trustees. Also includes trustees' distribution and orientation information.	Board Secretary	E + 2	-	E + 2	E + 1		PIB	Archival Review		E = expiry of term of office.	EA-O MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
HUM	Human Resources	The function of managing all employees within the organization in accordance with policies and procedures. Records include but are not limited to personnel records, employee collective agreements, employee information (including medical information), conditions of work, overtime, salary rates, pensions, benefits, payroll records, grievances, performance evaluations and recruitment.	Human Resources										
HUM	Attendance – Employee	Includes records regarding employee attendance, absences (leaves and sabbaticals) and vacations. Records include details about vacation schedules, hours of work, absenteeism reports and related reports from the HRIS systems.	Human Resources	E + 3		E + 3			PIB			E = date record created.	ESA-O MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
HUM	Criminal Background Checks	Includes records listing any criminal code convictions that have not been pardoned for all existing and new employees, service providers and volunteers that come into direct contact with students on a regular basis.	Human Resources	E	E + 6	E + 6	E		PIB			E = termination of employment or six years without an offence declaration for volunteers.	EA-O MFIPPA-O
HUM	Criminal Offence Declarations	Annual offence declarations, signed by the employee/service provider, which lists all criminal code convictions registered since the date of the CBC or last offence declaration.	Human Resources	S + 1		S + 1	C		PIB			Retain current and previous year.	EA-O MFIPPA-O
HUM	Staff Listings and Reports	Includes all report listings concerning staff, e.g., staff directories, seniority lists, retirement lists and lists of supply teachers.	Human Resources	S + 1	-	S + 1	S		PIB			S = when new lists are received.	MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
HUM	Employee Benefit Plans	Includes brochures, rates, quotes, correspondence and explanatory documents regarding benefits offered to employees such as group insurance, dental plans, employee assistance program, benefit rate changes and premium adjustments.	Human Resources	S + 1	-	S + 1	S						Operational value
HUM	Employee Incident/ Accident Reports	Includes reports of accident/injury to board/authority employees under the *Workplace Safety and Insurance Act* and designated substances exposure records under the Occupational Health and Safety Act. Records may include: doctor's notes, follow-up notes and related correspondence, and short-term and long-term disability claims for both teaching and support staff and record of	Human Resources	E + 1	6	E + 7	E		PIB			E = claim settled.	LA-O MFIPPA-O OHSA-O WSIA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		administration of first aid.											
HUM	Employee Records	Includes records regarding the employment history of the board/authority or school employees. Includes initial resume and applications, internal applications, benefit enrollment forms, salary calculation forms, change advice, employee master record cards, certification of level placement, probationary contract, key tasks, and employee verification forms. Includes teaching and support staff.	Human Resources	E + 1	6	E + 7	E	Vital	PIB			E = termination of employment.	LA-O OHSA-O MFIPPA-O WSIA-O
HUM	Employee Surveys	Includes surveys and research conducted on board/authority staff regarding issues and	Human Resources	S + 1		S + 1	S		PIB			S = when survey is updated.	MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		planning that affect them.											
HUM	Employment Equity Program	Includes records and historical information regarding employment equity.	Human Resources	E + 1	2	E + 3	E + 1		PIB	Archival Review		E = termination of the plan.	MFIPPA-O
HUM	Human Resource Planning	Includes records of succession planning, staff allocations, staff turnover, staff mobility, promotions, transfers and related records.	Human Resources	C + 1	4	C + 5	C + 1		PIB				MFIPPA-O
HUM	Job Descriptions	Includes job descriptions and specifications as well as background information used in their preparation or amendment. Also includes positions of responsibility.	Human Resources	S + 2	-	S + 2	S			Archival Review		S = when new job descriptions are written.	Operational value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
HUM	Labour Relations Negotiations and Agreements	Includes records regarding the administration and interpretation of the board's/authority's collective agreements and includes seniority lists, implementation plans, subplans, and related records. Also includes records related to collective bargaining, e.g., final offers, memoranda of settlement, mediations, arbitrations, and scatter grams used in preparation for bargaining. Excludes collective agreements. See **LEG**.	Human Resources	E + 5	-	E + 5	E					E = termination of contract period; seniority lists until suspended.	
HUM	Labour Relations: Grievances and Arbitration	Includes records regarding grievances filed by employees, such as evaluation reports, notifications, correspondence with unions concerning grievance initiators, and legal opinions.	Human Resources	E + 5	-	E + 5	E		PIB			E = resolution/withdrawal of grievance.	MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
HUM	Labour Relations: Union Certification	Includes original documents concerning the certification of labour unions.	Human Resources	P	-	P	P						
HUM	Medical Records: Hazardous Materials Exposure	Records of exposure to asbestos and other hazardous materials.	Human Resources	E + 1	19	E + 20	E		PIB			E = last record made.	OHSA-O MFIPPA-O
HUM	Medical Records: Employee	Includes doctor's notes, correspondence, and health reports related to an employee's medical situation.	Human Resources	E + 1		E + 1	E		PIB			Note: Maintain confidentially and limit access (OPSBA guidelines).	MFIPPA-O
HUM	Pay Equity	Includes records regarding the establishment and implementation of the board's/authority's pay equity plan. Records include background information, consultant information, questionnaires, interview documentation and job evaluation plans.	Human Resources	S + 1	4	S + 5	S						

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
HUM	Pension/ Superannuation Plans	Includes general information on OMERS, TPP and other annuity or superannuation plans and annual information returns.	Human Resources	S	Life of Board/ Authority	Life of Board / Authority	S						
HUM	Performance Appraisals	Includes records of job performance appraisals on all employees according to established timelines and criteria through board/ authority procedures.	Human Resources	E + 1	5	E + 6	E		PIB			E = date of appraisal.	MFIPPA-O EA-O
HUM	Professional Development Participation	Includes records relating to invitations, approvals and registrations for internal and external training events, seminars and workshops.	Originating Department	C + 1	-	2	C + 1		PIB				MFIPPA-O
HUM	Training Records	Includes records related to staff training mandated by legislation or board policy including confined space general and specific training, WHMIS training, etc.	Human Resources	S + 1	3	S + 4			PIB				MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
HUM	Professional Development Programs and Materials	Includes records regarding courses and conferences facilitated by the board/ authority for staff development and information on career and professional development programs. Also includes conference proceedings and presentations, orientation materials and staff development calendars.	Originating Department	C + 1	3	C + 4	C + 1			Archival Review			Operational value
HUM	Recruitment and Hiring	Includes records regarding the recruitment of staff. Includes job postings, copies of advertisements, competitions and resumes of candidates selected for interviews.	Human Resources	E + 1	-	E + 1	E			Archival Review		E + posting. Note: Only retain files for people interviewed.	Operational value
HUM	Resumes and Job Applications	Records include applications, resumes and applicant evaluations to support recruitment in the school and school board/ authority. Excludes resumes of candidates selected to be	Human Resources	E + 6M		E + 6M	E		PIB			E = decision regarding hiring or not. Resume is transferred to employee file upon hiring. (Suspend destruction for	MFIPPA-O Legal value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		interviewed.										grievances.)	
HUM	Salary Administration	Includes records regarding the planning and scheduling of salaries, such as job evaluations, job classification systems, salary surveys and schedules, salary increments, service pay and substitution pay. Excludes pay equity planning.	Human Resources	S	-	S + 1	S						
HUM	Staff Awards, Certificates and Bursaries	Includes records relating to special recognition and awards presented to staff.	Human Resources	C + 2	-	C + 2	C + 2		PIB			Subject to inclusion in the employee record.	MFIPPA-O
HUM	Temporary Resourcing	Includes correspondence, requests for temporary help, lists of floater secretaries/supply teachers, etc.	Human Resources	E + 1		E + 1	E	Vital	PIB			E = termination of employment.	MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
HUM	Volunteer Development	Includes records of volunteer programs such as recruitment workshops, annual receptions and volunteer activities in schools. Records include volunteer guidelines, correspondence, and volunteer program details. Excludes criminal background checks and offense declarations.	Schools	S		S + 1	S		PIB	Archival Review			MFIPPA-O
ICT	Information and Communications Technology	The function of applying and managing information and communications technology to support the business needs of the organization to capture, store, retrieve, transfer, communicate and disseminate information through automated systems such as Wide Area Networks and Local Area Networks. Includes planning, determining requirements, developing											

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		acquiring, modifying and evaluating applications and databases, and acquiring, tendering, leasing, licensing, registering and disposition of systems.											
ICT	Computer System and architecture Documentation	Records relating to the design of computer systems and/or software, including needs assessments, business cases, project charter, process flowchart documentation, impact analysis, user and system requirements, specifications, testing plans and results, user sign-offs, project management meeting minutes/documentation, system development documentation, software design records, and software inspection notes. Also includes records on system	ICT	S		S + 2	S					E = life of system.	

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		installations/conversions and product evaluations. May also include requests for significant modification, fixes and upgrades.											
ICT	Information Systems Production Activity and Control Files	Records relating to computer system operations and backup tapes. Includes activity logs, help desk tickets, change control sheets, change orders, file access control reports, system changes, and mainframe access forms.	ICT	S + 1		S + 1							
ICT	Access Control and Password Records	Records related to the management of and access to programs. Includes individual access, password management, etc.	ICT	E + 1		E + 1						E = termination of employee.	
ICT	Telecommunications Systems	Records relating to the management and maintenance and use of telecommunications equipment. Includes	ICT	E + 1	2	E + 3						E = life of system.	

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		system documentation, configuration details and services provided.											
LEG	Legal	The function of addressing legal issues relating to the operations of the board/ authority and **schools**. Records include, but are not limited to, claims and litigation files, appeals and hearings, contracts and agreements entered into on behalf of the board/ authority and schools, deeds and titles relating to properties, harassments incidents, etc.											
LEG	Accident/ Incident Claims and Reports	Includes reports related to student accidents that occur on board/authority property, schools and the administration offices or on school trips. Records include claims, communications, investigations, reports, administration of first aid and action taken as a	Business/ Corporate Services	E + 2	-	E + 2	E + 1		PIB			If applies to student, keep until student is age 18 and report is at least 2 years old.	MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		result of the accident. Includes reports to OSBIE. Excludes claims/ litigations, WSIB claims/ reports.											
LEG	Acts and Legislation/ Regulations	Includes single copies of Acts and Regulations, bills and judgments relevant to the board's/authority's activities, as well as correspondence and discussion papers concerning the Acts and Regulations and amendments to them.	Corporate Services	S + 1	-	S + 1	S					S = when act or regulation is replaced.	Operational value
LEG	Appeals/ Hearings	Includes records of hearings conducted with regard to issues that affect the school/board/ authority. Records include correspondence, reports, discovery findings, hearing proceedings and final decisions.	Originating Department /Legal	E	5	E + 5	E		PIB			E = final resolution.	LA-O MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
LEG	Claims/ Litigation	Includes all liability claims and litigation against or entered into by the boards/authorities and schools. Records include reports, correspondence, investigations, etc. Excludes accident reports and WSIB/STD/LTD claims .	Originating Department /Legal	E + 1	-	E + 1	E + 1		PIB			E = resolution of claim.	LA-O
LEG	Contracts and Agreements	Correspondence and information related to contracts and agreements.	Originating Department /Legal	E + 1	5	E + 6	E + 1			Archival Review		E = expiry of agreement.	LA-O
LEG	Deeds and Titles	Includes original deeds to any board-/authority-owned property.	Legal	Life of Board		Life of Board	Life of Board					*Registry Act/* *Land Titles A ct*	RPLA-O
LEG	Insurance Policies	Records relating to policies to cover loss or damage to property or premises and cover staff and general public against injury or death resulting from accidents on school/ board/authority premises	Legal	E + 1	5	E + 6	E + 1					E = expiry of policy.	LA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		or occurring during employment. Records include insurance policies, documentation regarding the annual review of insurance policies, certificates, appraisals and related correspondence. Excludes insurance claims and accident reports.											
LEG	Legal Opinions/ Precedents	Records relating legal opinions and precedents about legal issues identified by the school/board/authority. Records include case law, correspondence, reports, and findings/opinions provided to requestor.	Legal	E + 1		E + 1	E					E = completion of issue.	Operational value
LEG	Policing Arrangements	Includes correspondence between schools and police departments regarding extra duty officers, police visits to schools, and related items.	Originating Department	C + 1	-	C + 4	2						Operational value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
LEG	Property Acquisition and Sale	Includes land purchase agreements, development agreements, property appraisals, valuations and quotes concerning land owned by the board/ authority or under consideration for purchase. Also includes plans, correspondence, reports and backup documentation relating to the acquisition or sale of lands.	Originating Department	E + 1	19	E + 20	E + 1					E = disposal of property.	RPLA-O
LEG	Property Damage/ Trespassing Reports	Includes reports and general correspondence regarding property damage, theft or loss. Also includes vandalism reports, copies of repair invoices, monthly and annual summaries.	Originating Department	E + 1	4	5	1		PIB			E = date of damage.	RPLA-O MFIPPA-O
LEG	Incidents - Racial Discriminat ion and Harassmen	Includes records of incidents involving staff and students, incident reports, investigations, and correspondence	Originating Department	E + 1	-	E + 1	1		PIB		OS R		MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
	t	regarding these issues. Excludes appeals/hearings.											
PDD	Program Design and Development	The function of applying curriculum guidelines and designing education programs for students. Records include but are not limited to proposals, correspondence, lesson plans, and course outlines.											
PDD	Program Development and Design	Includes proposals, correspondence and curriculum development materials including writing projects teaching units, lesson plans, blank examinations, testing ideas, songs, games, music sheets and other learning materials.	Curriculum/ Program Services	S + 3	-	S+3	S + 1						CA-C EA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
PDD	Program Planning	Includes proposals for new curriculum program, either system-wide or at the school level. Includes meeting notes and reports. Also includes material regarding comparisons with programs in other school boards, provinces and countries. Includes program review reports and other valuations of specific programs in the curriculum. Also includes EQAO test results.	Curriculum/ Program Services	S + 3	-	S + 3	S + 1			Archival Review		E = last Ministry review or audit.	EA-O
PDD	Program/ Curriculum Guidelines	Includes Ministry/board/ authority guidelines, directives, approved texts and software lists, and related correspondence concerning the provision of specific programs in the curriculum (e.g., junior/senior kindergarten, French immersion).	Curriculum/ Program Services	S + 3	-	S+3	S + 1			Archival Review			CA-C EA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
PDD	Outlines/Courses of Study	Includes outlines of available programs and courses of study.	Curriculum/ Program Services	S + 3	-	S + 3	S + 1			Archival Review			CA-C
PSC	Programs and Services in the Community	The function of offering programs and services to the community through school and board/ authority facilities. Programs include night school and summer school, and services to the community include day care and safety awareness. Records include but are not limited to lesson units, reports, program reviews, teaching materials, correspondence and program brochures/ advertising. Generally refers to programs that are not part of day school.											

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
PSC	Programs and Services: Community	Includes records such as Education Week, summer arts camp, mentorship for Immigrants and community use of schools, day care services and safety and awareness programs. Also includes program reviews and reports of the activities of community liaison officers.	Curriculum/ Program Services	S + 1	3	C + 4	1			Archival Review			
PSC	Programs: Continuing Education	Includes objectives, lesson units, principal reports, program reviews, teaching materials and related records used in continuing education programs (such as heritage awareness, second language, multicultural, seniors programs).	Curriculum/ Program Services	S + 3		S + 3	S + 1			Archival Review			
PSC	Programs: Driver Education	Includes program outlines and correspondence concerning education in the safe operation of motor vehicles.	Curriculum/ Program Services	E + 1	3	E +1	E + 1		PIB			E = completion of the program.	MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
PSC	Programs: Parks and Recreation	Includes correspondence and records of programs such as swimming and fitness made available through municipal Parks and Recreation or the YMCA/YWCA.	Curriculum/ Program Services	1	-	1	1						
RPL	Research and Planning	The function of undertaking research and planning to support the ongoing operations of the school and board. Records include but are not limited to research surveys, studies and reports which address issues such as school boundaries, student demographics, municipal planning and statistics used to support Ministry funding requests.											
RPL	Planning: School Enrolments	Includes records regarding planning and development issues within the municipality that may have implications on enrolments within the school system. Includes	Originating Department	C + 1	3	C + 4	1						Operational value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		subdivision plans, official plan amendments, Ontario population reports, and traffic studies.											
RPL	Planning: School Boundaries	Includes information relevant to the establishment of school boundaries for purposes of enrolment and facility use. Includes boundary descriptions, school attendance areas and maps.	Originating Department	S	P	P	S			Archival Review			Operational value EA-O
RPL	Research Projects: School System	Includes records relating to internal and external research. Records include applications, surveys and research reports undertaken to capture information about school system issues; student evaluation and scoring systems and student backgrounds; school and career selection; and external research. Records include applications,	Originating Department	E + 1	5	E + 6	E + 1			Archival Review		E = completion of research project.	Operational value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		surveys and research reports.											
RPL	Research Projects: Curriculum /Program	Includes records of any research conducted into curriculum or program development, such as questionnaires, interest surveys and independent research studies.	Curriculum/ Program Services	E + 1	5		E + 1			Archival Review		E = completion of research project	Operational value
RPL	Research Requests: External	Includes external applications to conduct research from sources such as universities, graduate students, and foundations, and their final reports.	Originating Department	E + 1			E			Archival Review		E = completion of external research project.	Operational value
RPL	Strategic Planning	Includes all strategic and operational planning documents, and mandates, as well as	Originating Department	S + 2	-	S + 2	S + 1			Archival Review			Operational value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		related correspondence and background and reference information.											
RPL	Reference Materials	Includes information gathered as background data to support research and other activities within the board/authority and the school. Information may include articles, white papers, research reports, and information from other schools and boards.	Originating Department	S + 2	-	S + 2	S + 1						Operational value
RPL	Research Projects: Student Demographics	Includes aggregate reports profiling the characteristics of the student population, such as age, grade, promotion, and country of birth, religion, and other trend data.	Originating Department	E + 1	5	E + 6	E + 1			Archival Review			Operational value
STU	Student Services	The function of providing students with programs and services in accordance with the *Education Act*. Records cover such areas											

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		as admissions, transfers and withdrawals, Ontario Student Records, guidance and counselling, assessments, consent/ permission forms for special activities and programs, and extra-curriculum programs and participation. Records include but are not limited to student marks, program participation records, examination and testing records, and counselling records.											
STU	Bursaries and Awards	Includes records regarding bursaries and awards presented to students at commencement or graduation.	School	E + 1	-	E + 1	1		PIB		OSR	E = retirement/ transfer of student.	MFIPPA-O
STU	Case Files: Placement Assessments	Records relating to the assessments of students to determine their language background, immigration status, educational history and vocational testing.	School	E + 1		E + 1	E		PIB		OSR	E = retirement/ transfer of student.	MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
STU	Case Files: Attendance Issues	Includes records for students who are referred for counseling on attendance problems. Also includes SALEP records.	School	E + 1		E + 1	E		PIB		OSR	E = retirement/ transfer of student. Subject to inclusion in the OSR.	MFIPPA-O
STU	Case Files: Counselling	Includes case files of students who are referred for behavioural difficulties, psychological testing, speech and language issues, and social worker reports. Records include referrals, reports, and case notes.	School	E + 10		E + 10	E		PIB		OSR	Case files are maintained in accordance with Health Care Professional guidelines. E = date of last contact or date student turns 18 years of age. Copies of summary reports may be included in the OSR for retention in accordance with the OSR	MFIPPA-O EA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
												guideline.	
STU	Case Files: Referrals	Includes a compilation of all records for individual students who are referred for student services. Includes final summaries, confidential reports, and consents to disclosure and referral forms (e.g., IPRC). May include home instruction/home schooling records.	Student Services	E + 1		E + 1	E		PIB		OSR	E = resolution of issue. Subject to inclusion in the OSR. E = date of last contact or date student turns 18 years of age. Subject to inclusion in the OSR.	MFIPPA-O
STU	Case Files: Student Welfare	Includes correspondence and confidential reports regarding students where there is suspicion of child abuse, neglect or family violence.	School	E + 1		E + 1	1		PIB			E = date of report. This documentation is not considered part of the Ontario Student Record and should be kept in a file in the principal's office	MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
												for security. A notation that a report has been forwarded to the Children's Aid Society is adequate for the OSR. After most recent reports, retained only by special approval of the board/ authority.	
STU	Certificates of Program Completion	Records relating to successful completion of programs offered by the school/board/authority. Records include certificates and correspondence related to courses. Excludes report cards and day school program.	School	E + 1		E + 1	E		PIB		OSR	E = completion of course.	MFIPPA-O
STU	Examinations and Testing	Includes records regarding student exams and/or province-wide testing (e.g., EQAO). Records include correspondence,	School	C + 1	-	C + 1			PIB				MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		exam day schedules, exam day attendance and originals of completed student examinations. Excludes master copies of blank exams.											
STU	Extracurricular/ Co-curricular Activities	Includes records regarding school extracurricular activities such as clubs, choir, student council, and athletics.	School	C + 1	-	C + 1	C + 1						Operational value
STU	Guidance Materials	Includes brochures, calendars, description sheets and catalogues relating to career opportunities, external school programs, post-secondary education, private schools, and scholarships to support students.	School	S	-	S	S						Operational value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
STU	Office Index Cards	Includes all office index cards containing personal information, as well as retirement/transfer information on individual students, which is available for immediate access and as OSR backup information. The OIC may be retained electronically if a hard copy can be readily produced.	School	E + 55	-	E + 55	E + 1		PIB			E = retirement/transfer of student. Remains with school after E.	MFIPPA-O EA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
STU	Ontario Student Records (OSR)	Includes original Ontario Student Record folders with all documentation maintained for the OSR system, such as final student report cards and Ontario Student Transcripts, records of instruction in French/Native as a second language, documentation file, Special Education programs and SALEP. May include reports from third parties in accordance with the Ministry's Guideline if: • "the principal is of the opinion that the report is conducive to the improvement of the instruction of the student; • the principal receives written consent, from the adult student or the parent(s) or guardian(s) of a student who is not an adult, to the inclusion of the report."	School	E + 5	E + 50	E + 55	E + 1					E= retirement/transfer of student*, computer database record purged, on retirement/transfer. **Note**: Includes electronic data. **Note**: 5 years post-retirement, shred all records but the office index card, the transcript and the OSR folder in accordance with the OSR guideline. **Note**: Consult with SOE for identified students. Retention for Violent Incidents Report.– E + 3 or E + 5 (as	MFIPPA-O EA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		The information relating to suspension for violent behaviour shall not be removed from the OSR unless three consecutive years have passed during which no further suspensions for serious violent incidents have taken place. Excludes Office Index Cards.										below). No Suspension/No Expulsion – E + 3 (E = three years without report of a violent incident to police). Suspension – E + 3 (E = completion of three consecutive years during which there were no further suspensions for serious violent behaviour).	

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
												Expulsion – E + 5 (E = five years from the date of expulsion).	
STU	Programs: Co-operative Education	Includes correspondence with potential employers, surveys, and monthly monitoring teacher reports, statistics and other records of co-operative education programs. Also includes apprenticeship programs.	School	E + 1	5	E + 6	E + 1					E = termination of work placement.	120

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		Excludes Work Education Agreements.											
STU	Programs: Non-classroom	Includes records regarding student exchanges and field trips and arrangements for special events related to specific programs, such as concerts, festivals, track meets, facility tours, tournaments, art or essay contests, and science fairs. Records include correspondence, plans, schedules, etc.	School	C + 1	-	C + 1	C + 1			Archival Review			MFIPPA-O
STU	Registers: Student Enrolment and Attendance	Includes registers and reports concerning the enrolment/attendance of students, recording of daily attendance, and daily absence reports. Also includes class registers for non-school system programs such as	School	E + 1		E + 2	E		PIB	Archival Review		Retain for Ministry audit purposes. See Instructions for the Use of Computerized Enrolment Registers for Elementary and	MFIPPA-O EA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		continuing education, driver education and heritage language programs.										Secondary Schools. Requires printed copies of current and previous year's register.	
STU	Registers: Student Marks	Includes information on students' courses completed, marks received and mark verification sheets. Also includes electronic records. Excludes report cards.	School	C + 1					PIB			Student marks are included in OSR as part of report card.	MFIPPA-O
STU	Student Health Records	Includes medical and health information regarding students required for the care and treatment of students in the school setting. Includes pediculosis, medical emergency plans, administration of medication plans and other health related materials.	School	C + 1	-	C + 1			PIB		OSR	Subject to inclusion in OSR.	MFIPPA-O 214

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
STU	Student Meal Programs	Includes records of school milk and breakfast programs, such as lists of students involved in the programs.	School	C + 1	-	C + 1			PIB				MFIPPA-O
STU	Student Records: External Program Participation	Includes requests, consent/permission forms, correspondence and reports regarding school field trips and reports relating to the student(s) involved in student exchanges.	School	E + 1	-	E + 1	E		PIB	Archival Review	OSR	E = completion of exchange or program. Subject to inclusion in OSR.	MFIPPA-O
STU	Student Records: Continuing Education	Includes mature student appraisals, marks and other student-centred records for continuing education courses.	School	E + 1	-	E + 1	E		PIB		OSR	E = retirement/transfer of student.	MFIPPA-O
STU	Student Records: Co-op Programs	Includes records of individual students participating in co-operative education work assignments, such as copies of work education agreements, evaluation forms for employer interviews, training plans	School	E + 1	-	E + 1	E		PIB		OSR	E = retirement/transfer of student. Subject to inclusion in the OSR.	MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		and applications for programs, and student evaluation forms. Excludes co-operative education agreements.											
STU	Student Records: Specialized Equipment Needs	Includes records for students requiring special equipment to assist in the instruction of the student. Excludes financial records for ISA claims.	School	E + 1	-	E + 1	E		PIB		OSR	E = retirement/transfer of student. Subject to inclusion in the OSR.	MFIPPA-O
STU	Student Records: Special Program	Includes records of individual students who are referred for placement in special program classes, such as applications for admission, tests, assessments and raw data (e.g., IEP).	School	E + 1	-	E + 1	E		PIB		OSR	E = retirement/transfer of student. Subject to inclusion in the OSR.	MFIPPA-O
STU	Student Registrations/ Applications	Includes registration forms and applications for school entry or special programs such as French Immersion, summer school or continuing education. Also	School	S	-	S	S		PIB		OSR		MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		includes copies of applications to universities and colleges, etc.											
STU	Student Reporting	Includes all reports concerning individual students that are retrievable by student name or other identifier, such as first language reports, non-resident student reports, class list reports, Ontario Scholar lists, tape dumps, student online transaction listings and Student Information System edits.	School	E + 1	-	E + 1	E + 1		PIB				MFIPPA-O
STU	Suspensions/Expulsions	Includes records of students who are suspended/expelled from school and all school-related activities in accordance with the *Education Act.* Includes investigative notes, reports and appeal records.	School	E + 3	-	E + 3			PIB		OSR	E= incident of suspension, where no further suspensions have occurred. Final suspension letters may be filed in the OSR in accordance with board/	MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		Note: Special rules apply for retention of suspension letters for violent incidents.										authority policy. Records may be removed or retained by principal if deemed appropriate. Suspension for violent incidents to be retained as follows (per MOE Violence Free Schools Policy): E + 3 or E + 5 (as below) No Suspension/No Expulsion – E + 3 (E = three years without report of a violent incident to police).	

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
												Suspension – E + 3 (E = completion of three consecutive years during which there were no further suspensions for serious violent behaviour). Expulsion – E + 5 (E = five years from the date of expulsion).	
STU	Timetables /Schedules	Includes elementary course timetables, secondary school course calendars, yard duty schedules, school year calendars, school bell schedules, and related	School	S	-	S	S			Archival Review			Operational Value

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		records. Also includes timetables and "teacher day books" maintained by teachers. Excludes student timetables, course selection sheets, individual student exams and exam schedules.											
STU	Transfers/Exits/ Admittances/ Retirements/	Includes reports and forms recording the transfer, exit, room changes, promotions or admittance of students from schools. Also includes signed and dated forms authorizing student admissions, transfers or retirements.	School	E + 1	-	E + 1	E + 1		PIB			Subject to inclusion in the OSR.	MFIPPA-O
STU	Transportation: Student Bus Services	Includes records concerning transportation/busing for transportation of students to and from schools, Special Education, field trips, and special programs. Records include bus schedules, requests for transportation, bus	School	S + 1	-	S + 1	S + 1		PIB				MFIPPA-O

Classification			Retention Recommended Responsible Department and Retention (to be adjusted to reflect local school board/authority needs)					Vital Record	Personal Information Bank (MFIPPA requirement)	Archival Selection	Included in OSR	Notes/Reference	Value of record (operational, legal or based on retention period in law) Click on law short form to ink to the law in e-laws or CanLii.
Function	Record Series	Scope Notes/Function Description	Responsible Department (RD)	RD Retention Period Active	RD Retention Period Inactive	RD Total Retention Period	Non-Responsible Department Retention Period (copies, short term operation use)						
		routes, boundaries and student lists (names and addresses).											

Function	Record Series	Subject/Record Type
ADM	Associations/Organizations	Block Parents
ADM	Associations/Organizations	Community Organizations
ADM	Associations/Organizations	CPCO
ADM	Associations/Organizations	OASBO
ADM	Associations/Organizations	OCSTA
ADM	Associations/Organizations	Ontario School Counsellors' Association
ADM	Associations/Organizations	School Advisory Councils
ADM	Audio-Visual Services	Audio-Visual Bookings
ADM	Audio-Visual Services	Audio-Visual Requests
ADM	Audio-Visual Services	CanCopy
ADM	Audio-Visual Services	Distribution and Use of AV materials
ADM	Audio-Visual Services	Film Catalogue
ADM	Forms Inventory	Blank Forms
ADM	Library Management	Collection Titles
ADM	Library Management	Delivery Listings
ADM	Library Management	Library Holdings
ADM	Library Management	Library Operations
ADM	Library Management	Overdue Item Listings
ADM	Meeting Documentation: Internal	District Head Meetings
ADM	Meeting Documentation: Internal	Managers' Meetings
ADM	Meeting Documentation: Internal	Principals' Council
ADM	Meeting Documentation: Internal	Secretaries' Meetings
ADM	Meeting Documentation: Internal	Subject Head Meetings
ADM	Meeting Documentation: External	Accessibility Committee
ADM	Meeting Documentation: External	CODE
ADM	Meeting Documentation: External	MISA
ADM	Meeting Documentation: External	OASBO
ADM	Meeting Documentation: External	Ontario Public School Board Association
ADM	Meeting Documentation: External	PIMT
ADM	Meeting Documentation: External	Transportation Consortium

Function	Record Series	Subject/Record Type
ADM	Meeting Documentation: Internal	Department Meetings
ADM	Meeting Documentation: Internal	Liaison Committee Meetings
ADM	Meeting Documentation: Internal	Project Team Meetings
ADM	Records Destruction Notices	Destruction Authorization Notice
ADM	Records Destruction Notices	Lists of Destroyed Records
ADM	Records Management Listings and Reports	File Lists
ADM	Records Management Listings and Reports	Lists of Records in Storage
ADM	Records Management Listings and Reports	Records Management Program Outlines
ADM	Records Management Listings and Reports	Retention Schedules
ADM	Requests for Information	Access to Student Records
ADM	Requests for Information	Freedom of Information
ADM	Requests for Information	MFIPPA
ADM	Requests for Information	Requests for Information
ADM	Service Requisitions and Reports: Internal Services	Courier Services
ADM	Service Requisitions and Reports: Internal Services	Duplicating Services
ADM	Service Requisitions and Reports: Internal Services	Mail Services
ADM	Service Requisitions and Reports: Internal Services	Printing Services
ADM	Service Requisitions and Reports: Internal Services	Requests for Service - Duplicating
ADM	Service Requisitions and Reports: Internal Services	Requests for Service - Mail
ADM	Vendors/Suppliers/Contractors	Price Lists
ADM	Vendors/Suppliers/Contractors	Vendor Catalogues
ADM	Vendors/Suppliers/Contractors	Vendors and Suppliers Lists
COM	Advertisements	Advertisements
COM	Advertisements	JK/K Advertisements
COM	Advertisements	Recruitment Advertisements
COM	Advertisements	Tender Advertisements
COM	Appreciation and Commendations	Appreciation Letters
COM	Appreciation and Commendations	Certificates of Appreciation
COM	Appreciation and Commendations	Commendations
COM	Communiqués	Brochures (Program)

Function	Record Series	Subject/Record Type
COM	Communiqués	Outlines (Program)
COM	Communiqués	Program Brochures
COM	Communiqués	Program Outlines
COM	Complaints	School Activities
COM	Complaints	School Board/Authority Activities
COM	Contacts and Mailing Lists	Emergency Contact Lists
COM	Contacts and Mailing Lists	Mailing Lists
COM	Contacts and Mailing Lists	Parental Emergency Contact Lists
COM	Contacts and Mailing Lists	Student Lists
COM	Events, Ceremonies and Celebrations	Bake and Craft Sales
COM	Events, Ceremonies and Celebrations	Book Fairs
COM	Events, Ceremonies and Celebrations	Career Information Days
COM	Events, Ceremonies and Celebrations	Christmas Concerts
COM	Events, Ceremonies and Celebrations	Education Week
COM	Events, Ceremonies and Celebrations	Graduations/ Commencements
COM	Events, Ceremonies and Celebrations	Hot Dog Day
COM	Events, Ceremonies and Celebrations	New School Openings
COM	Events, Ceremonies and Celebrations	Parent's Night
COM	Events, Ceremonies and Celebrations	Recruitment Events
COM	Events, Ceremonies and Celebrations	Remembrance Day
COM	Events, Ceremonies and Celebrations	Retirements Receptions
COM	Media Kits, Communications and News Releases	Information Releases
COM	Media Kits, Communications and News Releases	Media Communications
COM	Media Kits, Communications and News Releases	Media Kits
COM	Media Kits, Communications and News Releases	News Releases
COM	Media Kits, Communications and News Releases	Press Releases
COM	Memorabilia	Board Memorabilia
COM	Memorabilia	Crests
COM	Memorabilia	School Histories
COM	Memorabilia	School Logos

Function	Record Series	Subject/Record Type
COM	Memorabilia	Songs
COM	Memorabilia	Uniforms
COM	Multimedia Materials	Audio Tapes
COM	Multimedia Materials	Class Photographs
COM	Multimedia Materials	Officials' Photographs
COM	Multimedia Materials	Photographs
COM	Multimedia Materials	Recordings
COM	Multimedia Materials	Slides
COM	Multimedia Materials	Trustee Photographs
COM	Multimedia Materials	Videotapes
COM	Multimedia Materials	Yearbook Photographs
COM	News Reports	News Clippings
COM	Publications: Internal	Annual Reports
COM	Publications: Internal	Artwork
COM	Publications: Internal	Curriculum Handbooks
COM	Publications: Internal	High School Booklets
COM	Publications: Internal	Newsletters
COM	Publications: Internal	Program Brochures
COM	Publications: Internal	Promotional Material
COM	Publications: Internal	School Calendars
COM	Publications: Internal	School Handbooks
COM	Publications: Internal	Yearbooks
COM	Speeches and Presentations	Presentations
COM	Speeches and Presentations	Speeches
COM	Website Content	Website Content
COM	Website Content	Website Snapshots
COM	Website Content	Websites
Dam	Audio Visual Services	Equipment Repair
FAC	Building and Site Approvals	Building Permits
FAC	Building and Site Approvals	Building Plan Approvals

Function	Record Series	Subject/Record Type
FAC	Building and Site Approvals	Municipal Reports
FAC	Building and Site Approvals	Site Plan Approvals
FAC	Confined Spaces	Confined Space Plan
FAC	Confined Spaces	Hazard Controls
FAC	Confined Spaces	Protective Equipment Use
FAC	Designated Substance and Hazardous Material Monitoring: Hazardous Biological, Chemical or Physical Agents	Air Quality Monitoring
FAC	Designated Substance and Hazardous Material Monitoring: Hazardous Biological, Chemical or Physical Agents	Air Quality Testing
FAC	Designated Substance and Hazardous Materials: Waste Monitoring and Management	Chemicals
FAC	Designated Substance and Hazardous Materials: Waste Monitoring and Management	Disposal of Chemicals
FAC	Designated Substance and Hazardous Materials: Waste Monitoring and Management	Disposal of Hazardous Waste
FAC	Designated Substance and Hazardous Materials: Waste Monitoring and Management	Hazardous Waste
FAC	Designated Substance and Hazardous Materials: Waste Monitoring and Management	Hazardous Waste Inventories
FAC	Drawings and Specifications	Addition Plans
FAC	Drawings and Specifications	Aerial Plans
FAC	Drawings and Specifications	Alteration Plans
FAC	Drawings and Specifications	Architects' Instructions
FAC	Drawings and Specifications	Building Code Requirements
FAC	Drawings and Specifications	Fire Code Requirements
FAC	Drawings and Specifications	Floor Plans
FAC	Drawings and Specifications	Maps
FAC	Drawings and Specifications	Mechanical, Electrical and Structural Specifications
FAC	Drawings and Specifications	Site Plans

Function	Record Series	Subject/Record Type
FAC	Drawings and Specifications	Technical Specifications
FAC	Emergency Plans	Business Continuity Plans
FAC	Emergency Plans	Emergency Preparedness
FAC	Emergency Plans	Fire Drill Guidelines and Plans
FAC	Emergency Plans	Strike Plans
FAC	Facilities Construction Projects	Capital Program Requests
FAC	Facilities Construction Projects	Ceiling Cost Formulas
FAC	Facilities Construction Projects	Certificates of Clearance
FAC	Facilities Construction Projects	Drawings and Plans
FAC	Facilities Construction Projects	Impact Statements
FAC	Facilities Construction Projects	Progress Reports
FAC	Facilities Construction Projects	School Building Projects
FAC	Facilities Improvement Projects	Building Additions
FAC	Facilities Improvement Projects	Building Alterations
FAC	Facilities Improvement Projects	Building Improvement Projects
FAC	Facilities Improvement Projects	Building Renovations
FAC	Facilities Planning	Allocation of Classrooms
FAC	Facilities Planning	Allocation of Student and Teacher Workspace
FAC	Facilities Planning	Physical Space Layouts
FAC	Facilities Planning	Portable Reports
FAC	Facilities Planning	Projected Use of Facilities
FAC	Facilities Planning	School Floor Plans
FAC	Facilities Planning	Space Planning
FAC	Facilities Planning	Space Utilization
FAC	Food Services/Cafeteria	Food Services/Cafeteria
FAC	Health and Safety Committee	Health and Safety Inspection Reports
FAC	Health and Safety Committee	Infestations
FAC	Health and Safety Committee	Joint Health and Safety Committee Agendas and Minutes
FAC	Incident Reports: Health and Safety and Student Safely	Infection Reports

Function	Record Series	Subject/Record Type
FAC	Incident Reports: Health and Safety and Student Safely	Quarantine Reports
FAC	Incident Reports: Health and Safety and Student Safely	Work Refusals
FAC	Inspection and Testing Logs and Reports: General	Elevator Contacts
FAC	Inspection and Testing Logs and Reports: General	Elevator Log Books
FAC	Inspection and Testing Logs and Reports: General	Elevator Requests for Service
FAC	Inspection and Testing Logs and Reports: General	Elevator Service Documentation
FAC	Inspection and Testing Logs and Reports: General	Playground Safety Reports
FAC	Inspection and Testing Logs and Reports: General	Spills, Leaks or Soil Contamination
FAC	Inspection and Testing Logs and Reports: General	Underground Tank Inspections
FAC	Inspection and Testing Logs and Reports: General	Water Management
FAC	Inspection and Testing Logs and Reports: General	Water Testing Reports
FAC	Inspection and Testing Logs and Reports: General	Well Reports
FAC	Inspection and Testing Logs and Reports: General	Workplace Inspections
FAC	Inspection Logs and Reports: Fire Protection Equipment and Emergency Power Systems	Emergency Power Inspection Reports
FAC	Inspection Logs and Reports: Fire Protection Equipment and Emergency Power Systems	Inspection Reports Fire Extinguishers
FAC	Inspection Logs and Reports: Fire Protection Equipment and Emergency Power Systems	Inspection Reports and Tag Portable Fire Extinguishers
FAC	Land Surveys	Construction Layouts
FAC	Land Surveys	Control Surveys
FAC	Land Surveys	Field Notes
FAC	Land Surveys	Property Surveys
FAC	Land Surveys	Soil Boring Reports
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	Air Conditioning
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	Classroom Equipment
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	Cleaning
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	Equipment Manuals

Function	Record Series	Subject/Record Type
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	Heating
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	Lawnmovers/Snowblowers
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	Office Equipment
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	Operational Equipment
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	Pool Operations
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	Requests for Equipment Maintenance
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	School Equipment
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	Shop Equipment
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	Steam Cleaners and Vacuums
FAC	Maintenance and Operations: Buildings/Physical Plant and Equipment	Ventilation
FAC	Maintenance and Operations: Grounds	Grounds Keeping
FAC	Maintenance and Operations: Grounds	Parking Management
FAC	Maintenance and Operations: Grounds	Pest Control
FAC	Maintenance and Operations: Grounds	Recycling
FAC	Maintenance and Operations: Grounds	Snow Clearance
FAC	Material Safety Data Sheets	Material Safety Data Sheets
FAC	Security	Emergency Telephone Numbers
FAC	Security	Key Control
FAC	Security	Police Station Locations
FAC	Security	Surveillance Reports
FAC	Security	Trespassing
FAC	Vehicles/Fleet Management	Vehicle History Files

Function	Record Series	Subject/Record Type
FAC	Vehicles/Fleet Management	Vehicle Maintenance Files
FAC	Vehicles/Fleet Management	Vehicle Registration
FIN	Accounts Payable	Cheque Requisitions
FIN	Accounts Payable	Employee Expenses
FIN	Accounts Payable	Gas Bills
FIN	Accounts Payable	Hydro Bills
FIN	Accounts Payable	Invoices
FIN	Accounts Payable	Legal Fees
FIN	Accounts Payable	Payment Vouchers
FIN	Accounts Payable	Permit Receipts
FIN	Accounts Payable	Petty Cash Disbursements
FIN	Accounts Payable	Phone Bills
FIN	Accounts Payable	Trustees Expenses
FIN	Accounts Payable	Vendor Transaction Listings
FIN	Accounts Receivable	Non-resident Fees
FIN	Accounts Receivable	Permit Revenue
FIN	Accounts Receivable	Records of Income from Fundraising events
FIN	Accounts Receivable	Reimbursements from Other Boards
FIN	Accounts Receivable	Student Tuition
FIN	Accounts Receivable	Transportation Fees
FIN	Audits: Financial	Financial Audits
FIN	Banking and Cash Management	Bank Reconciliations
FIN	Banking and Cash Management	Bank Statements
FIN	Banking and Cash Management	Cancelled Cheques
FIN	Banking and Cash Management	Cheque Stubs
FIN	Banking and Cash Management	Deposit Records
FIN	Banking and Cash Management	Money Order Rates
FIN	Banking and Cash Management	Signing Authorities
FIN	Budgets	Budget Formula Calculations
FIN	Budgets	Budgeted vs. Actual Reports

Function	Record Series	Subject/Record Type
FIN	Budgets	Capital Budgets
FIN	Budgets	Current Estimate Highlights
FIN	Budgets	Estimates and Revised Estimates
FIN	Budgets	Grant Calculations
FIN	Budgets	Operating Budgets
FIN	Budgets	Preliminary Formula Budgets
FIN	Capital Projects Financing	Budget Approvals
FIN	Capital Projects Financing	Building Monthly Costs
FIN	Capital Projects Financing	Capital Expenditure Forecasts
FIN	Capital Projects Financing	Capital Payment Vouchers
FIN	Capital Projects Financing	Costing
FIN	Capital Projects Financing	Quarterly Reports
FIN	Capital Projects Financing	Working Papers
FIN	Capital Revenue	Rental Income from Leased Premises
FIN	Capital Revenue	Sale of Property
FIN	Cost Allocations	Allocation of Costs to Other Schools
FIN	Cost Allocations	Allocation of Tuition to Other Schools
FIN	Financial Forecasts and Reports	Forecasts and Financial Reports
FIN	Financial Forecasts and Reports	GL Reports
FIN	Financial Forecasts and Reports	Variance Reports
FIN	Financial Forecasts and Reports	Yearly Schedules
FIN	Financial Statements	Application of Funds
FIN	Financial Statements	Audited Financial Statements
FIN	Financial Statements	Balance Sheets
FIN	Financial Statements	Income Statements
FIN	Financial Statements	Statement of Source
FIN	Financial Work Papers	Development of Financial Statements
FIN	Financial Work Papers	Grant Calculations
FIN	Funding Assessments	Analysis of Assessments and Mill Rates
FIN	Funding Assessments	International Visa Students

Function	Record Series	Subject/Record Type
FIN	Funding Assessments	Levies and Assessments
FIN	Funding Assessments	Non-resident Students
FIN	Funding: External Sources	Administration of Bequests
FIN	Funding: External Sources	Background Information
FIN	Funding: External Sources	Community Support Fund
FIN	Funding: External Sources	Copies of Wills
FIN	Funding: External Sources	Data Sheets
FIN	Funding: External Sources	Donations to the Board
FIN	Funding: External Sources	Fund Histories
FIN	Funding: External Sources	ISA Claims
FIN	Funding: External Sources	Provincial Grant Programs
FIN	Funding: External Sources	Scholarship Funds
FIN	Funding: External Sources	Transportation Subsidies
FIN	Funding: Student Council	Accounts Receivable and Payable
FIN	Funding: Student Council	Invoices
FIN	Funding: Student Council	Vouchers
FIN	Fundraising: Charitable Organizations	Charitable Organizations
FIN	Fundraising: Charitable Organizations	Easter Seals
FIN	Fundraising: Charitable Organizations	Fundraising
FIN	Fundraising: Charitable Organizations	Kidney Foundation
FIN	Fundraising: Charitable Organizations	United Way
FIN	Income Tax Returns	Annual Income Tax Return
FIN	Inventory Control: Fixed Assets	Fixed Assets
FIN	Inventory Control: Non-fixed Assets	Inventories of Board-owned Equipment
FIN	Investments	Board Investments
FIN	Investments	Bonds Issued
FIN	Investments	Debentures
FIN	Investments	Investments - Fuel for Later Sale
FIN	Investments	Payments to Investors
FIN	Investments	Promissory Notes

Function	Record Series	Subject/Record Type
FIN	Investments	Term Deposits
FIN	Journal Vouchers and Journal Entries	Journal Input Forms
FIN	Journal Vouchers and Journal Entries	Journal Vouchers
FIN	Journal Vouchers and Journal Entries	JV Background Documentation
FIN	Ledgers: General	Books of Original Entry
FIN	Ledgers: General	General Ledgers
FIN	Ledgers: Subsidiary and Journals	Payment and Receipt Journals
FIN	Ledgers: Subsidiary and Journals	Payroll Registers
FIN	Ledgers: Subsidiary and Journals	Purchase Order Registers
FIN	Ledgers: Subsidiary and Journals	Subsidiary Ledgers
FIN	Ledgers: Subsidiary and Journals	Subsidiary Registers
FIN	Ledgers: Subsidiary and Journals	Year-end Adjustment Registers
FIN	OnSIS Reporting	Enrolment Projections
FIN	OnSIS Reporting	March Reports
FIN	OnSIS Reporting	Ministry Reporting
FIN	OnSIS Reporting	October Reports
FIN	OnSIS Reporting	Statistical Reports For Ministry
FIN	Payroll Management	Billing Reports: Payroll
FIN	Payroll Management	Direct Deposit Requests
FIN	Payroll Management	Holdbacks
FIN	Payroll Management	Payroll
FIN	Payroll Management	Payroll Deduction Reports
FIN	Payroll Management	Payroll Master Cards
FIN	Payroll Management	Payroll Update Logs
FIN	Payroll Management	Salary Payments
FIN	Payroll Management	Timesheets
FIN	Payroll Management	Wage Deductions
FIN	Pension Contributions and Support	Contribution Cards
FIN	Pension Contributions and Support	OMERS Reports
FIN	Pension Contributions and Support	Superannuation Plans

Function	Record Series	Subject/Record Type
FIN	Pension Contributions/Support	Annuity Plans
FIN	Purchasing Documentation	Bid and Performance Bonds
FIN	Purchasing Documentation	Invitations to Tender
FIN	Purchasing Documentation	Product Selection Documentation
FIN	Purchasing Documentation	Proposals
FIN	Purchasing Documentation	Purchase Orders
FIN	Purchasing Documentation	Purchase Requisitions
FIN	Purchasing Documentation	Quotations and Tenders
FIN	Purchasing Documentation	Requests for Proposal
FIN	Purchasing Documentation	Requests for Quotation
FIN	Purchasing Documentation	Tender Submissions
FIN	Sales and Property Tax Returns and Reports	Federal Sales Tax
FIN	Sales and Property Tax Returns and Reports	Gas Surtax Reports
FIN	Sales and Property Tax Returns and Reports	Goods and Services Tax Returns
FIN	Sales and Property Tax Returns and Reports	Requests for Tax Rebates
FIN	Sales and Property Tax Returns and Reports	Tax Assessments
FIN	Transportation Reports and Costing	Bus Capacity Loading
FIN	Transportation Reports and Costing	Bus Cost Reports
FIN	Transportation Reports and Costing	Bus Route Costing
FIN	Transportation Reports and Costing	Fuel Rates
GOV	Appointments: Board and Committee	Auditor
GOV	Appointments: Board and Committee	Banking Authority
GOV	Appointments: Board and Committee	Board and Committee Appointments
GOV	Appointments: Board and Committee	Board Solicitor
GOV	Appointments: Board and Committee	Library Boards
GOV	Articles of Incorporation, By-laws and Constitution	Articles of Incorporation
GOV	Articles of Incorporation, By-laws and Constitution	By-laws
GOV	Articles of Incorporation, By-laws and Constitution	Constitution
GOV	Audits: Program	Curriculum Plan Audits
GOV	Audits: Program	Ministry Audits

Function	Record Series	Subject/Record Type
GOV	Audits: Program	Program Audits
GOV	Guidelines, Policies and Directives: External	EIC Guidelines
GOV	Guidelines, Policies and Directives: External	Ministry Directives
GOV	Guidelines, Policies and Directives: External	Ministry Guidelines and Directives
GOV	Guidelines, Policies and Directives: External	Ministry Memoranda
GOV	Guidelines, Policies and Directives: External	Ministry Policies
GOV	Guidelines, Policies and Directives: External	OSR Guideline
GOV	Guidelines, Policies and Directives: Internal	Accounting Procedures
GOV	Guidelines, Policies and Directives: Internal	Directives
GOV	Guidelines, Policies and Directives: Internal	Emergency Procedures
GOV	Guidelines, Policies and Directives: Internal	Evaluation Handbooks
GOV	Guidelines, Policies and Directives: Internal	Evaluation Procedures
GOV	Guidelines, Policies and Directives: Internal	Guidelines
GOV	Guidelines, Policies and Directives: Internal	Personnel and Attendance Reporting Procedures
GOV	Guidelines, Policies and Directives: Internal	Policies
GOV	Guidelines, Policies and Directives: Internal	Procedures
GOV	Intergovernmental Reporting and Communication	College of Teachers
GOV	Intergovernmental Reporting and Communication	Intergovernmental Correspondence
GOV	Intergovernmental Reporting and Communication	Intergovernmental Reports
GOV	Intergovernmental Reporting and Communication	Members of Parliament
GOV	Intergovernmental Reporting and Communication	OISE (Ontario Institute for Studies in Education)
GOV	Intergovernmental Reporting and Communication	Provincial Ministries
GOV	Intergovernmental Reporting and Communication	Universities and Colleges
GOV	Meetings: Board of Directors	Agendas
GOV	Meetings: Board of Directors	Briefs
GOV	Meetings: Board of Directors	Minutes
GOV	Meetings: Board of Directors	Reports
GOV	Meetings: Board of Directors	Resolutions
GOV	Meetings: Governance Committees and Councils	Ad Hoc Committees
GOV	Meetings: Governance Committees and Councils	Administrative Council

Function	Record Series	Subject/Record Type
GOV	Meetings: Governance Committees and Councils	Agendas
GOV	Meetings: Governance Committees and Councils	Board Committees
GOV	Meetings: Governance Committees and Councils	Employee Assistance Advisory Committee
GOV	Meetings: Governance Committees and Councils	Minutes
GOV	Meetings: Governance Committees and Councils	Reports
GOV	Meetings: Governance Committees and Councils	School Councils
GOV	Meetings: Governance Committees and Councils	Special Education Advisory Committee
GOV	Meetings: Governance Committees and Councils	Standing Committees
GOV	Meetings: Governance Committees and Councils	Steering Committees
GOV	Meetings: Governance Committees and Councils	Task Forces
GOV	Organization Structure	Board Profiles
GOV	Organization Structure	Organization Analysis
GOV	Organization Structure	Organization Charts
GOV	Organization Structure	School Profiles
GOV	Permits/Facility Bookings	Provincial Elections
GOV	Trustee Management	Clerk's Certificates
GOV	Trustee Management	Municipal Elections
GOV	Trustee Management	News Items re: Trustees
GOV	Trustee Management	Trustee Information
GOV	Trustee Management	Trustees Distribution Information
GOV	Trustee Management	Trustees Orientation Information
GOV	Trustee Management	Trustees Register
HUM	Attendance: Employee	Absence Reports
HUM	Attendance: Employee	Employee Attendance Reports
HUM	Attendance: Employee	Employee Vacations
HUM	Attendance: Employee	Hours of Work Reports
HUM	Attendance: Employee	HRIS System Reports
HUM	Attendance: Employee	Leaves of Absence
HUM	Attendance: Employee	Requests
HUM	Attendance: Employee	Schedules/Planners

Function	Record Series	Subject/Record Type
HUM	Criminal Background Checks	Criminal Code Convictions
HUM	Criminal Offence Declarations	Annual Offence Declarations
HUM	Employee Benefit Plans	Benefit Brochures
HUM	Employee Benefit Plans	Benefit Quotes
HUM	Employee Benefit Plans	Benefit Rate Changes
HUM	Employee Benefit Plans	Benefit Rates
HUM	Employee Benefit Plans	Dental Plans
HUM	Employee Benefit Plans	Employee Assistance Program
HUM	Employee Benefit Plans	Group Insurance
HUM	Employee Benefit Plans	Premium Adjustments
HUM	Employee Claims	Long-Term Disability
HUM	Employee Claims	Short-Term Disability
HUM	Employee Incident/Accident Reports	WSIB
HUM	Employee Records	Applications
HUM	Employee Records	Benefit Enrolment Forms
HUM	Employee Records	Certification of Level Placement
HUM	Employee Records	Change Advices
HUM	Employee Records	Employee Master Record Cards
HUM	Employee Records	Employee Verification Forms
HUM	Employee Records	Key Tasks
HUM	Employee Records	Probationary Contracts
HUM	Employee Records	Records of Employment
HUM	Employee Records	Resumes
HUM	Employee Records	Salary Calculation Forms
HUM	Employee Surveys	Surveys and Research
HUM	Employment Equity Program	Employment Equity Plans
HUM	Human Resource Planning	Allocation of Staff
HUM	Human Resource Planning	Staff Allocation
HUM	Human Resource Planning	Staff Mobility
HUM	Human Resource Planning	Staff Placement

Function	Record Series	Subject/Record Type
HUM	Human Resource Planning	Staff Promotions
HUM	Human Resource Planning	Staff Transfers
HUM	Human Resource Planning	Staff Turnover
HUM	Human Resource Planning	Succession Planning
HUM	Job Descriptions	Job Descriptions
HUM	Job Descriptions	Position Descriptions
HUM	Job Descriptions	Positions of Responsibility
HUM	Labour Relations: Grievances and Arbitration	Evaluation Reports
HUM	Labour Relations: Grievances and Arbitration	Grievances
HUM	Labour Relations: Grievances and Arbitration	Notifications
HUM	Labour Relations: Grievances and Arbitration	Union Correspondence
HUM	Labour Relations: Negotiations and Agreements	Administration of Collective Agreements
HUM	Labour Relations: Negotiations and Agreements	Arbitrations
HUM	Labour Relations: Negotiations and Agreements	Collective Agreements
HUM	Labour Relations: Negotiations and Agreements	Implementation Plans
HUM	Labour Relations: Negotiations and Agreements	Mediations
HUM	Labour Relations: Negotiations and Agreements	Memoranda of Settlement
HUM	Labour Relations: Negotiations and Agreements	Negotiations
HUM	Labour Relations: Negotiations and Agreements	Scatter Grams
HUM	Labour Relations: Negotiations and Agreements	Seniority Lists
HUM	Labour Relations: Union Certification	Labour Union Certification
HUM	Medical Records: Employee	Health Reports and Assessments
HUM	Medical Records: Employee	Doctor's Notes
HUM	Medical Records: Hazardous Materials Exposure	Asbestos Reports
HUM	Medical Records: Hazardous Materials Exposure	Hazardous Material Exposure
HUM	Pay Equity	Consultant Information
HUM	Pay Equity	Interview Documentation
HUM	Pay Equity	Job Evaluation Plans
HUM	Pay Equity	Pay Equity Background Information
HUM	Pay Equity	Pay Equity Plan

Function	Record Series	Subject/Record Type
HUM	Pay Equity	Questionnaires
HUM	Pension/Superannuation Plans	Annual Information Returns
HUM	Pension/Superannuation Plans	Annuity Plans
HUM	Pension/Superannuation Plans	OMERS
HUM	Pension/Superannuation Plans	Superannuation Plans
HUM	Pension/Superannuation Plans	TPP
HUM	Performance Appraisals	Job Performance Appraisals
HUM	Performance Appraisals	Performance Appraisals
HUM	Professional Development Participation	Approvals for Courses
HUM	Professional Development Participation	Course Registrations
HUM	Professional Development Participation	Invitations to Courses
HUM	Professional Development Participation	Seminars and Workshops: External
HUM	Professional Development Participation	Seminars and Workshops: Internal
HUM	Professional Development Programs and Materials	Career Development Programs: Staff
HUM	Professional Development Programs and Materials	Course Materials
HUM	Professional Development Programs and Materials	Professional Development Programs: Staff
HUM	Professional Development Programs and Materials	Session Descriptions
HUM	Recruitment and Hiring	Applicant Evaluations
HUM	Recruitment and Hiring	Competitions
HUM	Recruitment and Hiring	Job Advertisements
HUM	Recruitment and Hiring	Job Postings
HUM	Resumes and Job Applications	Job Applications
HUM	Resumes and Job Applications	Resumes
HUM	Salary Administration	Job Classification Systems
HUM	Salary Administration	Job Evaluations
HUM	Salary Administration	Salary Increments
HUM	Salary Administration	Salary Planning
HUM	Salary Administration	Salary Scheduling
HUM	Salary Administration	Salary Surveys
HUM	Salary Administration	Service Pay

Function	Record Series	Subject/Record Type
HUM	Salary Administration	Substitution Pay
HUM	Staff Awards, Certificates and Bursaries	Staff Awards
HUM	Staff Awards, Certificates and Bursaries	Staff Bursaries
HUM	Staff Awards, Certificates and Bursaries	Staff Certificates
HUM	Staff Listings and Directories	Lists of Supply Teachers
HUM	Staff Listings and Directories	Retirement Lists
HUM	Staff Listings and Directories	Seniority Lists
HUM	Staff Listings and Directories	Staff Directories
HUM	Temporary Resourcing	Keyboarding Tests
HUM	Temporary Resourcing	Lists of Floater Secretaries
HUM	Temporary Resourcing	Practice Teachers
HUM	Temporary Resourcing	Request for Temporary Help
HUM	Temporary Resourcing	Student Teachers
HUM	Temporary Resourcing	Summer Students
HUM	Temporary Resourcing	Supply Teachers
HUM	Training Records	First Aid Training
HUM	Training Records	WHIMS
HUM	Volunteer Development	Criminal Background Check
HUM	Volunteer Development	Offense Declaration
HUM	Volunteer Development	Recruitment Workshops
HUM	Volunteer Development	Volunteer Activities
HUM	Volunteer Development	Volunteer Annual Receptions
HUM	Volunteer Development	Volunteer Guidelines
HUM	Volunteer Development	Volunteer Programs
ICT	Access Control and Password Records	Access Control Matrix
ICT	Access Control and Password Records	Software Control
ICT	Computer System Design and Architecture	Computer Hardware and Software License Agreements
LEG	Accident/Incident Claims and Reports	Administration Offices
LEG	Accident/Incident Claims and Reports	Board Property

Function	Record Series	Subject/Record Type
LEG	Accident/Incident Claims and Reports	School Property
LEG	Accident/Incident Claims and Reports	School Trips
LEG	Accident/Incident Claims and Reports	Student Accidents
LEG	Acts and Legislation	Acts
LEG	Acts and Legislation	Amendments to Regulations
LEG	Acts and Legislation	Bills
LEG	Acts and Legislation	Discussion Papers
LEG	Acts and Legislation	Judgments
LEG	Acts and Legislation	Legislation
LEG	Acts and Legislation	Municipal By-laws
LEG	Acts and Legislation	Official Plans
LEG	Acts and Legislation	Regulations
LEG	Appeals and Hearings	Board Hearings
LEG	Appeals and Hearings	Closing of Schools
LEG	Appeals and Hearings	Final Decisions
LEG	Appeals and Hearings	FOI Appeals
LEG	Appeals and Hearings	Hearing Proceedings
LEG	Appeals and Hearings	Human Rights Appeals
LEG	Appeals and Hearings	IPRC Appeals
LEG	Appeals and Hearings	Ministry of Education Hearings
LEG	Appeals and Hearings	Official Hearings
LEG	Appeals and Hearings	Pay Equity Appeals
LEG	Appeals and Hearings	Student Suspension Appeals
LEG	Claims/Litigation	Discovery Reports
LEG	Claims/Litigation	Human Rights Claims
LEG	Claims/Litigation	Liability Claims
LEG	Claims/Litigation	Litigation Files
LEG	Contracts and Agreements	Bus Operators
LEG	Contracts and Agreements	Computer Hardware and Software License Agreements

Function	Record Series	Subject/Record Type
LEG	Contracts and Agreements	Equipment Rental and Service Contracts
LEG	Contracts and Agreements	Leases
LEG	Contracts and Agreements	Provincial Government
LEG	Contracts and Agreements	Purchase Agreements
LEG	Contracts and Agreements	Use of Grants
LEG	Contracts and Agreements	Vehicle Leases
LEG	Contracts and Agreements	Work Education Agreements for Coop Programs
LEG	Deeds and Titles	Deeds
LEG	Deeds and Titles	Titles
LEG	Incidents: Racial Discrimination And Harassment	Racial Discrimination
LEG	Incidents: Racial Discrimination And Harassment	Sexual Harassment
LEG	Incidents: Racial Discrimination and Harassment	Discrimination Incidents
LEG	Incidents: Racial Discrimination and Harassment	Harassment Incidents
LEG	Incidents: Racial Discrimination and Harassment	Racial Incidents
LEG	Insurance Policies	Adjusters' Premiums
LEG	Insurance Policies	Agents' Premiums
LEG	Insurance Policies	Insurance Appraisals
LEG	Insurance Policies	Insurance Certificates
LEG	Insurance Policies	Insurance Liabilities
LEG	Insurance Policies	Insurance Policies
FAC	Legal Opinions/Precedents	Legal Opinions/Precedents
FAC	Permits/Facility Bookings	Applications for Permits
FAC	Permits/Facility Bookings	Community Events
FAC	Permits/Facility Bookings	Federal Elections
FAC	Permits/Facility Bookings	Interjurisdictional Permits
FAC	Permits/Facility Bookings	Lists of Permit Holders
FAC	Permits/Facility Bookings	Permits for Use of School Property
FAC	Permits/Facility Bookings	Polling Stations
LEG	Policing Arrangements	Community Liaison Officers
LEG	Policing Arrangements	Extra Duty Officers

Function	Record Series	Subject/Record Type
LEG	Policing Arrangements	Police Visits to Schools
LEG	Property Acquisition and Sales	Acquisition of Lands
LEG	Property Acquisition and Sales	Correspondence
LEG	Property Acquisition and Sales	Development Agreements
LEG	Property Acquisition and Sales	Land Purchase Agreements
LEG	Property Acquisition and Sales	Plans
LEG	Property Acquisition and Sales	Property Appraisals
LEG	Property Acquisition and Sales	Reports and Backup Documentation
LEG	Property Acquisition and Sales	Sale of Lands
LEG	Property Acquisition and Sales	Valuations and Quotes
LEG	Property Damage/Trespassing Reports	Copies of Repair Invoices
LEG	Property Damage/Trespassing Reports	Loss Reports
LEG	Property Damage/Trespassing Reports	Monthly and Annual Summaries
LEG	Property Damage/Trespassing Reports	Property Damage Reports
LEG	Property Damage/Trespassing Reports	Theft Reports
LEG	Property Damage/Trespassing Reports	Vandalism Reports
LEG	Transportation Accidents: Bus	Accident Follow-up
LEG	Transportation Accidents: Bus	Accident Reports
LEG	Transportation Accidents: Bus	Bus Accident Communications
PDD	Outlines/Courses of Study	Available Programs
PDD	Outlines/Courses of Study	Courses of Study
PDD	Outlines/Courses of Study	Program Outlines
PDD	Program Development and Design	Blank Examinations
PDD	Program Development and Design	Curriculum Development Materials
PDD	Program Development and Design	Games
PDD	Program Development and Design	Learning Materials
PDD	Program Development and Design	Lesson Plans
PDD	Program Development and Design	Music Sheets
PDD	Program Development and Design	Songs
PDD	Program Development and Design	Teaching Units

Function	Record Series	Subject/Record Type
PDD	Program Development and Design	Testing Ideas
PDD	Program Development and Design	Writing Projects
PDD	Program Planning	EQAO Test Results
PDD	Program Planning	Program Evaluations
PDD	Program Planning	Program Review Reports
PDD	Program Planning	Programs in Other Schools
PDD	Program Planning	Teacher Day Book
PDD	Program/Curriculum Guidelines	Approved Texts
PDD	Program/Curriculum Guidelines	French Immersion Programs
PDD	Program/Curriculum Guidelines	Junior/Senior Kindergarten Programs
PDD	Program/Curriculum Guidelines	Ministry Curriculum Directives
PDD	Program/Curriculum Guidelines	Ministry Curriculum Guidelines
PDD	Program/Curriculum Guidelines	Software Lists
PSC	Programs and Services: Community	Community Use of Schools
PSC	Programs and Services: Community	Day Care Services
PSC	Programs and Services: Community	Mentorships
PSC	Programs and Services: Community	Safety and Awareness Programs
PSC	Programs: Continuing Education	Heritage Awareness
PSC	Programs: Continuing Education	Multicultural
PSC	Programs: Continuing Education	Night School
PSC	Programs: Continuing Education	Second Language
PSC	Programs: Continuing Education	Seniors' Programs
PSC	Programs: Continuing Education	Summer School
PSC	Programs: Driver Education	Driver Education Programs
PSC	Programs: Parks and Recreation	Fitness Programs
PSC	Programs: Parks and Recreation	Municipal Parks and Recreation
PSC	Programs: Parks and Recreation	Swimming Programs
PSC	Programs: Parks and Recreation	YMCA/YWCA
RPL	Planning: School Boundaries	Boundary Descriptions
RPL	Planning: School Boundaries	School Attendance Areas

Function	Record Series	Subject/Record Type
RPL	Planning: School Boundaries	School Maps
RPL	Planning: School Enrolments	Official Plan Amendments
RPL	Planning: School Enrolments	Planning and Development Issues
RPL	Planning: School Enrolments	Population Reports
RPL	Planning: School Enrolments	Subdivision Plans
RPL	Planning: School Enrolments	Traffic Studies
RPL	Reference Materials	Articles
RPL	Reference Materials	Research Reports
RPL	Reference Materials	White Papers
RPL	Research Curriculum/Program Research	Questionnaires
RPL	Research Data and Work Papers	Background Research and Data for Research Reports and Activities
RPL	Research Projects: Curriculum/Program	Curriculum Development Research
RPL	Research Projects: Curriculum/Program	Interest Surveys
RPL	Research Projects: School System	Applications
RPL	Research Projects: School System	External Research Reports
RPL	Research Projects: School System	External Surveys
RPL	Research Projects: School System	School and Career Selection Surveys
RPL	Research Projects: School System	School System Surveys
RPL	Research Projects: School System	Scoring System Surveys
RPL	Research Projects: School System	Student Background Surveys
RPL	Research Projects: School System	Student Evaluation Surveys
RPL	Research Projects: School System	Surveys
RPL	Research Projects: Student Demographics	Aggregate Reports: Student Population
RPL	Research Requests: External	Research Final Reports
RPL	Research Requests: External	Research Requests from Foundations
RPL	Research Requests: External	Research Requests from Graduate Students
RPL	Research Requests: External	Research Requests from Universities
RPL	Strategic Planning	Background Research Information
RPL	Strategic Planning	Strategic Plans

Function	Record Series	Subject/Record Type
STU	Bursaries and Awards	Commencement Awards
STU	Bursaries and Awards	Graduation Awards
STU	Bursaries and Awards	Student Bursaries and Awards
STU	Case Files: Attendance Issues	Attendance Counselling Records
STU	Case Files: Attendance Issues	Counseling Records: Attendance
STU	Case Files: Communications	Counseling Records: Communications
STU	Case Files: Counselling	Confidential Notes
STU	Case Files: Counselling	Interview Notes
STU	Case Files: Counselling	Psychological Testing/Assessment and Reporting
STU	Case Files: Counselling	Social Worker Referral Forms
STU	Case Files: Counselling	Speech and Language Issues
STU	Case Files: Counselling	Statistical Forms
STU	Case Files: Counselling	Social Worker Counselling and Reports
STU	Case Files: Placement Assessments	Assessment Test Results
STU	Case Files: Placement Assessments	Educational History
STU	Case Files: Placement Assessments	Immigration Status
STU	Case Files: Placement Assessments	Language Background Assessments
STU	Case Files: Placement Assessments	Recommendations for Levels of Placements
STU	Case Files: Placement Assessments	Vocational Assessments
STU	Case Files: Placement Assessments	Vocational Counselling Records
STU	Case Files: Placement Assessments	Vocational Interest Tests
STU	Case Files: Placement Assessments	Vocational Interview Notes
STU	Case Files: Referrals	Communication Counselling
STU	Case Files: Referrals	Confidential Reports
STU	Case Files: Referrals	Consents to Disclosure
STU	Case Files: Referrals	Final Summaries
STU	Case Files: Referrals	Home Instructions
STU	Case Files: Referrals	Home Schooling Records
STU	Case Files: Referrals	Referral Forms
STU	Case Files: Student Welfare	Abuse, Neglect, Family Violence

Function	Record Series	Subject/Record Type
STU	Examinations and Testing	Completed Student Examinations
STU	Examinations and Testing	EQAO
STU	Examinations and Testing	Exam Day Attendance
STU	Examinations and Testing	Exam Day Schedules
STU	Examinations and Testing	Student Exams
STU	Extracurricular/Co-curricular Activities	Athletics
STU	Extracurricular/Co-curricular Activities	Choir
STU	Extracurricular/Co-curricular Activities	Clubs
STU	Extracurricular/Co-curricular Activities	School Extracurricular Activities
STU	Extracurricular/Co-curricular Activities	Student Council
STU	Guidance Materials	Career Information
STU	Guidance Materials	College Information
STU	Guidance Materials	External School Programs
STU	Guidance Materials	Post-secondary Education
STU	Guidance Materials	Private Schools
STU	Guidance Materials	Scholarships
STU	Office Index Cards	Index Cards
STU	Office Index Cards	Retirement Information
STU	Office Index Cards	Transfer Information
STU	Ontario Student Records (OSR)	Ontario Student Records (OSR) Current
STU	Ontario Student Records (OSR)	Ontario Student Records (OSR) Retired Pupils
STU	Programs: Cooperative Education	Co-op Programs
STU	Programs: Cooperative Education	Co-op Statistics
STU	Programs: Cooperative Education	Employer Surveys
STU	Programs: Cooperative Education	Monitoring Teacher Reports
STU	Programs: Non-Classroom	Art
STU	Programs: Non-Classroom	Concerts
STU	Programs: Non-Classroom	Essay Contests
STU	Programs: Non-Classroom	Facility Tours
STU	Programs: Non-Classroom	Festivals

Function	Record Series	Subject/Record Type
STU	Programs: Non-Classroom	Science Fairs
STU	Programs: Non-Classroom	Tournaments
STU	Programs: Non-Classroom	Track Meets
STU	Programs: Student Meals	Student Lists
STU	Registers: Student Enrolment and Attendance	Continuing Education Registers
STU	Registers: Student Enrolment and Attendance	Daily Absence Reports
STU	Registers: Student Enrolment and Attendance	Daily Attendance Registers
STU	Registers: Student Enrolment and Attendance	Heritage Language Program Registers
STU	Registers: Student Enrolment and Attendance	Student Attendance Registers
STU	Registers: Student Enrolment and Attendance	Student Enrolment Registers
STU	Registers: Student Marks	Mark Verification Sheets
STU	Registers: Student Marks	Student Marks
STU	Student Assessments: Immigrants	Immigrant Assessments
STU	Student Exchanges	Student Exchange Reports
STU	Student Exchanges	Student Exchange Schedules
STU	Student Health Records	Health Information
STU	Student Health Records	Health Unit Information
STU	Student Health Records	Medical Information
STU	Student Meal Programs	Breakfast Programs
STU	Student Meal Programs	Lunch Programs
STU	Student Meal Programs	Milk Programs
STU	Student Records: External Program Participation	Plans for Student Exchanges
STU	Student Records: Continuing Education	Continuing Education Student Marks
STU	Student Records: Continuing Education	Mature Student Appraisals
STU	Student Records: Co-op Programs	Apprenticeship Programs
STU	Student Records: Co-op Programs	Co-operative Work Assignments
STU	Student Records: Co-op Programs	Copies of Work Education Agreements
STU	Student Records: Co-op Programs	Employer Interview Evaluation Forms
STU	Student Records: Co-op Programs	Program Applications
STU	Student Records: Co-op Programs	Student Evaluation Forms

Function	Record Series	Subject/Record Type
STU	Student Records: Co-op Programs	Training Plans
STU	Student Records: External Program Participation	Field Trips
STU	Student Records: External Program Participation	School Field Trips
STU	Student Records: External Program Participation	Student Exchange Programs
STU	Student Records: External Program Participation	Student exchanges
STU	Student Records: Special Needs	Special Equipment For Students
STU	Student Records: Special Program	Applications for Admission
STU	Student Records: Special Program	Assessments
STU	Student Records: Special Program	IEP Raw Data
STU	Student Records: Special Program	Tests
STU	Student Registrations/Applications	Application Forms
STU	Student Registrations/Applications	Continuing Education Applications
STU	Student Registrations/Applications	French Immersion Applications
STU	Student Registrations/Applications	Registration Forms
STU	Student Registrations/Applications	Special Program Applications
STU	Student Registrations/Applications	Student Registrations/Applications
STU	Student Registrations/Applications	Summer School Applications
STU	Student Reporting	Class List Reports
STU	Student Reporting	First Language Reports
STU	Student Reporting	Homeroom Lists
STU	Student Reporting	Non-resident Student Reports
STU	Student Reporting	Ontario Scholar Lists
STU	Student Reporting	Promotion Listings
STU	Student Reporting	Student Information System Reports
STU	Student Reporting	Student Online Transaction Listing
STU	Suspensions/Expulsions	Expulsion Notice
STU	Suspensions/Expulsions	Suspension Notice
STU	Timetables/Schedules	Course Timetables
STU	Timetables/Schedules	School Bell Schedule
STU	Timetables/Schedules	School Year Calendar

Function	Record Series	Subject/Record Type
STU	Timetables/Schedules	Teacher's Day Book
STU	Timetables/Schedules	Teacher's Timetables
STU	Timetables/Schedules	Yard Duty
STU	Transfers/Exits/Admittances/Retirements	Admittances
STU	Transfers/Exits/Admittances/Retirements	Exits
STU	Transfers/Exits/Admittances/Retirements	Retirements
STU	Transfers/Exits/Admittances/Retirements	Transfers
STU	Transportation: Student Bus Services	Boundaries
STU	Transportation: Student Bus Services	Bus Routes
STU	Transportation: Student Bus Services	Bus Schedules
STU	Transportation: Student Bus Services	Requests for Transportation
STU	Transportation: Student Bus Services	Student Lists

Function	Record Series	Subject/Record Type

PURPOSE

These guidelines are to encourage Ontario school boards/authorities to include key elements in either a privacy protection policy and/or procedure when these are first being created or when being revised.

Note: This document is a guideline only and is not intended in any way to be a legal opinion or to provide legal counsel.

The following are a list of guidelines that should be considered by Ontario school boards/authorities when drafting privacy policies:

1. A privacy policy should have as its objectives the protection of personal information under the control of the school board/authority and the right of privacy with respect to personal information that is collected, used, disclosed, and retained in the school system.
2. A comprehensive policy would include a clear definition of "Personal Information," "Consent," "Notice," "Retention," "Disclosure," "Access," "Security," "Collection," "Accuracy," and any other definitions that may provide clarity to wording in the policy.
3. The policy should be accessible in both language and scope. It is important to be clear and concise so that information can be communicated and understood by interested parties both internal and external to the organization.
4. A privacy policy should be consistent with policies within the organization.
5. The policy should be accompanied by a procedure that can be implemented and monitored.
6. A policy should contain sufficient detail so as to provide an outline of a school board's/authority's expectations for maintaining privacy to enable the public regulatory bodies, such as privacy commissioners or other organizations, to understand its compliance with legal standards.
7. A policy should contain a reference to school board/authority administrative procedures and/or other related policies.
8. The guiding principles of the policy can be drawn from the Ontario School Board/Authorities Privacy Standard:
    i. The school board/authority is responsible for personal information under its custody or control and shall designate an individual(s) in writing who is/are accountable for the school board's/authority's compliance with privacy legislation.
    ii. The purposes for which personal information is collected shall be specified, in conjunction with the legal authority for the collection, and the title, business address, and telephone number of an individual who can answer questions about the collection, and individuals shall be notified at or before the time personal information is collected except where otherwise permitted by law.
    iii. An individual's informed consent is required for the collection, use, or disclosure of personal information, except where otherwise permitted by law.
    iv. The collection of personal information is fair, lawful, and limited to that which is necessary for the specified purpose.
    v. The use, retention, and disclosure of personal information are limited to the specified purpose identified to the individual, except where otherwise permitted by law.

vi. School boards/authorities ensure that personal information is accurate, complete, and up-to-date in order to fulfill the specified purpose for its collection, use, disclosure, and retention.

vii. Personal information is secured and protected from unauthorized access, disclosure, and inadvertent destruction by adhering to safeguards appropriate to the sensitivity of the information.

viii. Policies and practices relating to the management of personal information are made readily available to the public.

ix. An individual has the right of access to his/her personal information and shall be given access to that information in accordance with privacy legislation, subject to any restrictions. An individual has the right to challenge the accuracy and completeness of the information and request that it be amended as appropriate or to have a letter/statement of disagreement retained on file. An individual to whom the disclosure has been granted in the year preceding a correction has the right to be notified of the correction/statement. An individual is advised of any third party service provider requests for his/her personal information in accordance with privacy legislation.

x. An individual may address or challenge compliance with the principles.

9. The school board/authority may also wish to include in the policy specific directives for:

i. The designation of the "Head" and for the delegation of responsibilities for accountability under the legislation.

ii. The development of administrative procedures that will provide for the protection of personal information under the control of the school board/authority.

iii. The development of administrative procedures that would facilitate the right of access to personal information and the right to challenge the accuracy and completeness of the information.

10. The school board/authority may also wish to reference within policy, relevant legislation, standards, and guidelines, including:

- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- Education Act
- Personal Health Information Protection Act (PHIPA)
- Personal Information and Protection of Electronic Documents Act (PIPEDA)
- The Ontario Student Record Guideline
- The Ontario School Boards and Authorities Privacy Standard

PURPOSE

The purpose of this template is to provide users with a document modeling a set of minimum requirements for a privacy policy. School boards/authorities may adapt and include other elements into a privacy policy document as determined by local needs and circumstances such as Special Education Services. This may include more detailed guidelines for specific departments, such as special education, which would also be consistent with the school board/authority privacy policy.

Policy

It is the policy of (name of school board/authority) to collect, use, retain and disclose personal information in the course of meeting its statutory duties and responsibilities. The school board/authority is committed to the protection of privacy and complies with all applicable provisions in the *Education Act*, the *Municipal Freedom of Information and Protection of Privacy Act*, the *Personal Health Information Protection Act*, and any other applicable legislation.

Rationale

The (name of school board/authority) only collects personal information when it is necessary for providing for the education for students and/or the employment of school board/authority employees or as required and authorized by law. The school board/authority operates under the authority of the *Education Act* and its associated regulations.

The management of personal information collected by the school board/authority for these purposes is in accordance with the provisions of the *Education Act*, the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), and the *Personal Health Information Protection Act* (PHIPA).

Guidelines

The protection of personal information held by the school board/authority is guided by the principles contained in the Ontario School Board/Authorities Privacy Standard.

1. **Accountability and Responsibility**

   Under MFIPPA, the school board/authority is responsible for personal information under its control and may designate in writing an individual(s) within the school board/authority who is accountable for compliance with privacy legislation.

   Under PHIPA, health information custodians are responsible for personal health information in their custody and control and may designate an individual within their school board/authority as an agent to assist with compliance to privacy legislation.

2. **Specified Purposes**

   The school board/authority shall identify the purpose(s) for which personal information is collected, and individuals shall be notified of the purposes and any other information required by law at or before the time personal information is collected.

3. **Consent**

   Personal information is collected for the provision of educational services to students. The knowledge and, in some cases, the consent of an individual is required for the collection, use, retention, and disclosure of personal information, except where otherwise permitted by law.

4. **Limiting Collection**

   The school board/authority shall limit the collection of personal information to that which is necessary for its specified purposes in accordance with its statutory duties and responsibilities.

5. **Limiting Use, Retention, and Disclosure**

   The school board/authority shall not use, retain, or disclose personal information for purposes other than those for which it was collected, except with the consent of the individual or as authorized or required by law. The school board/authority shall retain personal information in accordance with the school board/authority retention schedule.

6. **Accuracy**

   The school board/authority shall ensure that personal information is accurate, complete, and up-to-date in order to fulfill the specified purposes for its collection, use, disclosure, and retention.

7. **Safeguards**

   The school board/authority shall ensure that personal information is secured and protected from unauthorized access, use, disclosure, and inadvertent destruction by adhering to safeguards appropriate to the sensitivity of the information.

8. **Openness and Transparency**

   The school board/authority shall make available to the public specific information about its policies and practices relating to the management of personal information.

9. **Access and Correction**

   Upon request, the school board/authority shall allow an individual to access his/her personal information and will be given access to that information in accordance with privacy legislation, subject to any mandatory or discretionary exceptions. An individual has the right to challenge the accuracy and completeness of the information and to request that it be amended as appropriate or to have a letter/statement of disagreement retained on file. Any individual to whom the disclosure of the personal information has been granted in the year preceding a correction has the right to be notified of the correction/statement. An individual is advised of any third party service provider requests for his/her personal information in accordance with privacy legislation.

10. **Compliance**

    An individual shall have the ability to address or challenge compliance with these principles and in accordance with the school board's/authority's guideline/procedure.

Administrative Procedures

The Director of Education is authorized to provide the administrative procedures necessary to implement this policy.

PURPOSE

These guidelines relate to the issue of the right and appropriateness of sharing student information between a secondary school and the elementary schools that feed it.

Introduction

In 2004, direction was sought from the Information and Privacy Commission (IPC) about sharing student information back and forth between elementary and secondary school panels within one school board/authority. This guidance was necessary because an interpretation of section 266 of the Education Act was limiting the school boards'/authorities' ability to share in this way. This section says that student records are privileged to select employees of the school.

The interpretation and application of cross-panel sharing of personal student information must be done with care and respect in order to strike a balance between individual privacy rights and the practical provision of educational services. Students' information is collected and maintained on an individual basis for the improvement of instruction and every use must maintain that standard.

The IPC supported the request to broaden the interpretation of s. 266 with the understanding that parents/guardians and students be informed through a clear notice describing the personal student information that will be shared and including the contact information of a staff member who can answer questions. It was also recommended that this notice be provided to all new students upon registration.

This guideline describes the analysis undertaken as well as some suggestions for implementing compliant means of cross-panel personal information sharing.

Background

- Issue surfaced relative to inquiries related to new technologies and access to student level information
- Interpretation was explained and direction sought from the Information and Privacy Commissioner (IPC)
- Letter from Brian Beamish, Director of Policy and Compliance, IPC:
  - It is permissible to share individualized student data, including Ontario Student Record (OSR), and performance data between elementary and secondary schools.
  - Students and parents/guardians must be reasonably informed through a clear notice. The notice must describe the personal information, explain the purpose of the sharing, and provide a contact person's information. Notice must also be provided to new students upon registration.

Statutory Explanation

Reviewing the provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) explains why cross-panel sharing is an acceptable practice for the purposes of transition.

s53 (1): "This Act prevails over a confidentiality provision in any other Act unless the other Act or this Act specifically provides otherwise." *The Education Act does not, in s. 266 which covers OSRs, specifically provide for paramountcy over MFIPPA; therefore we must look to MFIPPA for access/use/disclosure instructions. (The majority of the data involved in transition is OSR data.) The authority of MFIPPA alters previously held understandings around student data management.*

s28 (2): "No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity." *Education Act ss.265 and 266 authorizes collection to create a student record.*

s29 (1): "An institution shall collect personal information only directly from the individual to whom the information relates unless.... another manner of collection is authorized by or under a statute." *Consent and notice are equal provisions under MFIPPA. (There is no hierarchy within the provisions.)*

s29 (2): "if personal information is collected on behalf of an institution, the head shall inform the individual to whom the information relates of:

- **a)** the legal authority for the collection;
- **b)** the principal purpose or purposes for which the personal information is intended to be used; and
- **c)** the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection." *This notice alerts families who prefer to exclude their children from activities, but by contacting the key person provided in the notice, we should be able to reduce exclusions to a minimum.*

Sections 31 and 32 cover the use and disclosure of personal information and list the key points:

"An institution shall not use/disclose personal information in its custody or control except:

- **a)** if the person to whom the information relates has identified that information in particular and consented to its use/disclosure;
- **b)** for the purpose for which it was obtained or compiled or for a consistent purpose;
- **c)** if the disclosure is made to an officer or employee of the institution who needs it in the performance of his/her duties and if the disclosure is necessary and proper in the discharge of the institution's functions. *The use of this data for transition purposes meets the requirements of b) and c) so long as we provide sufficient notifications. The vast majority of "uses" of student personal information are necessary to the provision of education services and are in keeping with our responsibilities under the Education Act and regulations, making notice sufficient.*

S34 (1): "A head shall make available for inspection by the public an index of all personal information banks in the custody or under the control of the institution, setting forth, in respect of each personal information bank,

- **a)** its name and location;
- **b)** the types of personal information maintained in it;
- **c)** how the personal information is used on a regular basis;

d) to whom the personal information is disclosed on a regular basis;

e) the categories of individuals about whom personal information is maintained; and

f) the policies and practices applicable to the retention and disposal of the personal information."
Posting this on your corporate site is an excellent way to communicate this publicly.

S35 (1): "A head shall attach or link to personal information in a personal information bank,

a) a record of any use/disclosure of that personal information for a purpose other than a purpose described in clause 43 (1) (d)." *Remember to track this for annual reporting purposes (as required by the Information and Privacy Commission).*

Drafting the Notice of Collection

This notice will contain:

1. Statement of Authority - "Student information is collected and used pursuant to the Education Act."
2. Purpose Statement - "Student information is shared between elementary and secondary schools for the purpose of easing transition. Programming can be adapted based on the information gathered."
3. Contact Information - Enough demographic information to allow contact with a person who understands and can explain the transition process.
4. Data Description - What personal student information is shared in advance of the student arrival at secondary school and what is shared with the student's former elementary school.

Communicating the Collection Notices

Two styles of collection notices should be used: a generic one on registration forms and a more explanatory notice in letters home, newsletters, websites, etc.

Notification Samples

1. Letters home, school/board websites and student agenda planners -

   "As students progress from elementary school to secondary school, important information is shared which eases a student's transition to secondary school. Sharing it also improves our ability to program effectively to the benefit of all students. Select student information will be shared at different times as required. This is authorized under the Education Act. Please note that all information used for the transition process is limited, secure and protected at all times. Please contact a Coordinating Superintendent of Education if you would like more information about the transition process - add contact details here."

2. Elementary and Secondary Registration Forms -

   "Student personal information is collected during registration and while attending school pursuant to the Education Act. It will be used for planning and programming, school to home communications, and to establish the Ontario Student Record which contains information conducive to the improvement of instruction. Limited information may be disclosed beyond the board for purposes such as yearbooks and accident information to the board's insurer. Questions about the information collected on this form should be directed to the principal of the school."

Things to Watch For

1. If families question the value of data sharing at transition:

   Express to families in positive terms that the notice is a courtesy and that there is zero risk. The sharing advantages their children.

2. Timing of "sharing":

   For the sharing of elementary data to the secondary panel, time it with the completion of the secondary registration form and/or the course selection form indicating the student's intention to attend a specific school.

   The timing of returning student data to the feeder elementary school is contingent on the nature of the program and resultant records, for example achievement data.

Some examples of transitioned personal information include, but are not limited to:

1. Student information provided to a secondary school in advance of a student's arrival:

Student Demographics:

- Student Name
- Date of Birth
- Board Student Number
- Ontario Education Number
- Gender
- Current Home Room
- Current Grade
- Special Education Status/Identification/Program Placement
- ESL/ELD stage or level / Program Delivery

Student Achievement:

- Report Card Achievement
- Report Card Learning Skills
- EQAO Results
- PM Benchmark and DRA reading level and/or other reading assessments

Student Attendance

Other Information:

- Suspensions/Expulsions
- Country of Birth
- Language Spoken at Home

2. Information about a student's performance in secondary school provided to the former elementary school:

   EQAO Grades 9 and 10 Results

   Report Card Achievement Data

   Credit Accumulation

   Course Selection

Alternatives to Cross Panel P.I. Sharing

1. Share school level data only
   a) Is personal information essential to the purpose?
   b) Can we achieve the same or very similar results sharing school level data only?
   c) What prevents us from using school level data only?
2. Depersonalize by removing identifiers (for example names)
   a) Does depersonalizing negatively impact the purpose?
   b) Can the purpose be split into two tiers – personalized and depersonalized?
   c) Even for "at-risk" students, how is managing depersonalized information going to impact the quality of what is learned from it?
   d) Depersonalized student information can be viewed by teachers who never actually teach that student; teachers who may be able to work better to the benefit of other students as a result.
3. Seek and acquire limited and specific signed parent/guardian consent in those instances where personal information is the only information we want and use
   a) Determine how often and for how long the information is needed and stays accurate.
   b) Prepare a consent form taking these things into consideration or add to existing forms (course selection and registration).

In Summary

MFIPPA has paramouncy over the *Education Act* relative to transition data sharing. In other words the direction comes from *MFIPPA* and not the *Education Act* because it lacks an express confidentiality provision.

Sharing student data is an internal administrative use managed by the Act and not, as the *Education Act* would have it, an external disclosure requiring much more stringent controls.

The Office of the Information and Privacy Commissioner of Ontario has required that clear notice be provided to affected families. This notice describes the information to be shared, contact information in case there are concerns and is to be provided to every affected student.

This document is a guideline only and is not intended in any way to be a legal opinion or to provide legal counsel

PURPOSE

This guideline defines and recommends best practices for managing recorded confidential records and information held by school boards/authorities. Following these practices will help to prevent breaches of privacy, security, or confidentiality. School boards/authorities should use this guideline to develop their own practices and procedures governing confidential records and information management.

Confidential

Recorded confidential records and information management refers to records and information that must be maintained in confidence and must not be disclosed unless authorized. Confidential records and information management includes but is not limited to private personal information. Confidentiality as a concept applies to a duty to protect records and information and can be applied to various types of records and information, not just personal records and information.

Disclosure of recorded confidential records and information should be limited to specific people or groups for a specific purpose. For example, this means that employees who require confidential records and information in the performance of their assigned duties–or, in the case of personal records and information, with the consent of the individual to whom the records and information relates–can indeed have it.

The Legal Framework

The *Ontario Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) provides a framework for determining which records and information may be considered as personal and/or confidential. The *Education Act* sets out, among other things, which information causes trustee meetings to be held in private session and which student information is private.

Personal and Confidential Records and Information

School board/authority records and information that may be confidential includes:

- a draft of a by-law;
- records and information revealing the substance of deliberations of a closed meeting, provided the closing of the meeting to the public is authorized by statute (*Education Act*);
- advice or recommendations of an officer or employee of an institution or a consultant retained by an institution;
- records and information received in confidence from government;
- records and information that disclose a trade secret or scientific, technical, commercial, financial, or labour relations records and information, supplied in confidence implicitly or explicitly (information falling in this definition must be treated as confidential in the absence of consent from the third party who provided it to the school board/authority;

- records and information that may be protected by legal privilege which includes:
  - communications between solicitor and client for the purposes of furnishing or obtaining legal advice (solicitor/client privilege);
  - records prepared in contemplation of or for use in litigation (litigation privilege); and
  - records prepared by or for legal cousel for use in giving advice.
- records and information protected by statutory privilege, i.e., the *Education Act* applies a statutory privilege to the Ontario Student Record (OSR) which restricts its use to the principal, superintendent, and teachers of the school for the improvement of the instruction of the pupil, unless consent is given by the adult student or the parent of the minor student for its broader use and disclosure;
- records and information collected by a health professional (e.g., psychologist, social worker, therapist) and/or clergy where specific circumstances are met;
- records and information that may pose a danger to safety or health; records and information that could reasonably be expected to seriously threaten the safety or health of an individual; refusing to disclose records and information to a parent when precluded to do so by court order or when in the principal's judgment there is an immediate risk of harm to a student.
- law enforcement records and information/proceedings (may include administrative tribunals);
- economic and other school board/authority interests, including:
  - trade secrets or financial, commercial, scientific, or technical records and information of a vendor or of the school board/authority;
  - records and information obtained through research by an employee, if the disclosure could reasonably be expected to deprive the employee of priority of publication;
  - records and information whose disclosure could reasonably be expected to prejudice the economic interests or the competitive position of the school board/authority;
  - records and information whose disclosure could reasonably be expected to be injurious to the financial interests of the school board/authority;
- positions, plans, procedures, criteria, or instructions to be applied to any negotiations carried on or to be carried on by or on behalf of the school board/authority;
- plans relating to the management of personnel or the administration of the school board/authority that have not yet been put into operation or made public;
- proposed plans, policies, or projects of the school board/authority if the disclosure could reasonably be expected to result in premature disclosure of a pending policy decision or undue financial benefit or loss to a person;
- questions that are to be used in an examination or test for an educational purpose.

Personal Information

Personal information is defined by MFIPPA as recorded information about an identifiable individual and should be treated as confidential unless it is public information or unless the individual consents to its disclosure or disclosure of the information is otherwise permitted by MFIPPA. For example, under MFIPPA, public information includes information that identifies an individual in a business or official capacity.

Personal Health Information which is a category of personal information should also be treated as confidential in accordance with the Personal Health Information Protection Act (PHIPA) where appropriate.

Identifying and Labeling Recorded Confidential Records and Information

Confidential records and information must be identified and clearly marked to ensure that staff can apply appropriate protection measures to the records and information. Marking may be done by including "CONFIDENTIAL" in the header or footer or as a watermark on all documents. Additionally, confidential documents or reports may be photocopied on coloured paper designated for that purpose, e.g., minutes of closed session on blue paper. Distribution or circulation of the documents may be restricted by including which persons may use the documents on each document, e.g., CONFIDENTIAL - for the use of the Board of Trustees only.

Only records that meet the criteria for confidential records and information should be marked as such. The following are some examples of confidential records and information:

- Reference letters
- Ontario Student Records
- Personnel records
- Evaluations of performance
- Health records
- Grievance files
- Appeal files
- Payroll records

When Could Records and Information Cease to Be Confidential?

Some confidential records and information may only be sensitive for specified periods, ceasing to be confidential after a certain period of time or change of circumstances. Here are some examples:

- RFP submissions.
- Draft press releases.
- Restructuring plans, policies, or projects.
- Personal information where it is about a person who has been dead for more than 30 years.

Access to Confidential Records and Information

Access to recorded confidential records and information is determined by the content of the records and information. MFIPPA allows an employee or agent of the organization who needs the records and information in the performance of his/her duties to have access to personal and confidential records and information on a limited, need-to know basis. School boards/authorities should assess the duties and responsibilities of each role to determine what information the staff member should be granted access to. Access to personal information should be minimized as much as possible to reduce risk.

Guidelines to Protect Confidential Records and Information

The following guidelines should be considered for confidential records:

- Access to the confidential records should be restricted only to those employees that require the records and information in the performance of their assigned duties.
- Include "confidential" in the header or footer or as a watermark or stamp for each document containing confidential records and information.
- Photocopying confidential reports on a coloured paper designated for that purpose, e.g., closed session minutes and agendas on blue paper.
- Keeping records in a secure location, such as in locked file cabinets, in locked rooms, or on a secure server. Cabinets should always be kept locked when not in use and located in a private/secure area, and access to the cabinets should be limited to authorized employees.
- Confidential records and information should be placed in a file folder, envelope, or other form of cover when out of the secure cabinet. When the record is not in use, it should be returned to the cabinet right away.
- Confidential records and information should never be left in an open area such as in an in-basket or on a desk. The record should be returned to the cabinet when not in use.
- Confidential records and information must be destroyed by secure shredding or by other secure data destruction methods.
- Confidential records and information should be stored separately from other similar records to support controlled access.
- For electronic records, store confidential records in separate directories or files, restrict access to these directories or files, and remove by secure deletion only.
- Computer screens should be positioned to prevent unauthorized viewing.
- Use passwords to protect confidential records and information and protect your passwords (see Password Guidelines).
- Shut down programs or use password protection on your computer when you leave your desk.
- Turn off your computer when leaving your desk for a long period of time.
- Shred drafts when they are no longer useful, and delete drafts from your computer.

- If you have confidential records on a notebook or laptop computer, ensure that either the documents themselves or the system are password protected. Do not leave your laptop in an easily accessible area where it could be stolen. Consider using data encryption for protected confidential records and information on portable devices.
- When travelling with confidential records, do not leave them unattended in vehicles, hotel or meeting rooms. Do not work with confidential records where others can see them.
- Do not remove Ontario Student Records from the school.
- If confidential records and information must be faxed, include a fax transmittal page with a confidentiality statement. Verify that the number on the screen is accurate before proceeding with the transmission, and confirm receipt of the documents.

Guidelines for the Secure Disposal of Confidential Records and Information

Confidential records and information must be disposed of securely to ensure they are permanently destroyed or erased in an irreversible manner and by a method that ensures that the records cannot be reconstructed in any way. When disposing of confidential records and information, official files as well as duplicate copies of documents made for in-office use should be considered.

- Paper - destruction means cross-cut shredding; this method is preferred to strip shredding, from which documents may be reconstructed. Consider whether on-site or off-site destruction is more suitable for your organization.
- Electronic and wireless media (such as floppy disks, CDs, USB keys, personal digital assistants (PDAs), and hard drives) - destruction means either physically damaging the item (rendering it unusable) and discarding it, or, if re-use within the organization is preferred, this entails employing file-wiping utilities provided by various software companies. Wiping may not, however, irreversibly erase every bit of data on a drive (see Information Technology Equipment Hardware Disposal and Redistribution Guidelines).

Resources

For more information on disposing of confidential records and information, refer to the Information and Privacy Commissioner of Ontario's Fact Sheet Number 10, *Secure Destruction of Personal Information*, available at http://www.ipc.on.ca/images/Resources/up-fact_10_e.pdf.

References

Information and Privacy Commissioner of Ontario's Fact Sheet Number 10, *Secure Destruction of Personal Information*, available at http://www.ipc.on.ca/images/Resources/up-fact_10_e.pdf.

York University, *Tip Sheet 2: Confidential Records*, available at http://www.yorku.ca/secretariat/infoprivacy/infotoolkit/docs/TipSheet2ConfidentialRecords.pdf.

Athabasca University, Guidelines - *Confidential Records and Information*, available at http://www.athabascau.ca/foipp/guidelines/guideline3.html.

PURPOSE

The effective management of passwords is the first line of defense in the electronic security of an organization. In a school board/authority environment it is not uncommon for most employees to have multiple passwords for access to email, voice mail, computer applications, and portals. Every school board should have a password strategy in place as part of the overall security strategy.

This document is intended to be used as a guideline for developing a password procedure. It contains considerations and strategies that can be used to develop procedures for the creation and maintenance of secure passwords.

Benefits of a Password Procedure

- Appropriate access for all staff;
- Effective identity management and access auditing;
- Preservation and protection of personal information entrusted to your care;
- Protection of YOUR personal information.

Best Practices/Recommendations

The successful adoption of a password procedure depends on the ability of the organization to enforce it. Some school boards/authorities have sophisticated technologies that can provide substantial automation and support for a large number of users. Others may have limited resources and will need to develop a procedure that is manageable in a more manual fashion. It is important to realize that regardless of which category the school board/authority falls into, password procedures are still a requirement for effective security management.

When creating a password procedure, it is important to consider elements that can be enforced through software security settings and those which must be enforced through education of the users. Items such as the minimum length of a password and expiry cycle for passwords are typically set through system software. Issues that would be linked to user education include not having passwords displayed on sticky notes and not sharing passwords.

Another important consideration when developing a password procedure is password retention. Even with the best procedures in place, passwords will be shared or otherwise become known over time, weakening security, so it is necessary to change them on a regular basis. Most systems allow the system administrator to set a parameter which causes passwords to expire and requires them to be reset by the user. This parameter is typically set for anywhere from 30 days to 90 days, depending on the number of users, level of risk, and manageability of the procedure. Password expiry does add some additional workload for technical staff as users often forget their new passwords and need support to change them. It is also wise to force a password reset the first time a user logs in to any system.

Technical Considerations

- **Length of password** - Passwords should be a minimum of six characters for adequate protection but should not be too long as to be onerous for staff to remember.
- **Mixed characters** - Passwords should contain at least one of the following: upper- and lower-case letters, numbers, and special characters (@#$!% etc). Where technology does not permit enforcement of this recommendation, it should be included in the user education.
- **Password retention** - Passwords should be reset on a regular basis and should expire after a set length of time. This can vary from 30 days to twice per year and will vary depending on the school board/authority culture and the technical support available.
- **Histories** - Password histories should be maintained and set so that users cannot use the same password twice within a defined period. The minimum history should be three passwords, but can be as high as the school board/authority chooses to set it.

User Education

For the users' protection, passwords created should be difficult to guess. The following points provide some guidance on best practices for creating a password:

- The password should not be the same as the username, even with a number or symbol added.
- Passwords should not contain personal information such as street number or name, company name, date of birth, etc.
- Passwords should never contain names of family members, pets, friends, or co-workers.
- Passwords shouldn't be a common phrase followed by a digit that is changed when the password expires.

Users should always follow these principles:

- Do not share passwords with anyone. If there is an issue that requires you to do so, remember to change the password immediately after the issue has been resolved.
- Never use the same password for work accounts as the one you have for personal use (banking, etc.).
- Do not write down passwords or include them in an email.
- Do not store passwords electronically unless they are encrypted.
- Never use the "Remember Password" feature on any systems; this option should be disabled in systems where technically feasible.

The following are some examples of both strong and weak passwords:

Password	Strength	Reason
Wam4uG	Good	Six characters, upper case and a number
sunny	Weak	Too short, too easy to hack/guess
charles1	Weak	User's first name used - too easy
22965	Weak	Same as user's personal banking PIN - poses additional risks to user
3z2tt4cy	Very Good	System-generated password which is changed every three months

Conclusion

There are many things to consider when developing a password procedure. Strict password procedures ensure greater security but require more user support and may result in a low compliance rate. Very relaxed password policies will likely result in higher compliance by users but may not provide adequate protection for school board/authority information. The key to an effective password procedure is to define a balance between the security needs of the school board/authority and its culture and to follow the guidelines defined here.

There are many valuable resources available online which can be used in conjunction with this document. The SANS (SysAdmin, Audit, Network, Security) Institute, www.sans.org, offers a password policy template that can be modified by an organization. Many school boards/authorities in Ontario have developed password policies or procedures and most are willing to share with other school boards/authorities.

PURPOSE

The use of mobile technologies in the course of daily work is becoming very common for school board/authority employees. Mobile devices can enhance the quality of work and life for employees, but they also dramatically increase the risk for data loss and personal information disclosure. The following guideline is intended to assist school boards/authorities in identifying areas of risk involving mobile devices and provide strategies for the development of an internal procedure or regulation.

Overview

When working both at the office or school and offsite, school board/authority employees must comply with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). The Act requires that organizations protect the privacy of individuals with respect to personal information about the individual held by the organization. This Act can be found at the Information and Privacy Commissioner's website: http://www.ipc.on.ca.

This guideline reflects best practices for securing mobile devices owned by a school board/authority, including but not limited to laptop computers, jump drives, cell phones, and PDAs, along with the personal information stored on these devices. The first principle of privacy is accountability. When personal information is in the care and/or custody of school board/authority employees, they are personally responsible for ensuring that privacy is protected.

Data owned by a school board/authority is not to be maintained or stored on any personally owned mobile devices. The major recommendations are:

- Personal information, to the greatest extent possible, should not be stored on mobile devices.
- Personal information, if stored on mobile devices owned by a school board/authority, should be:
  - Password-protected and/or securely encrypted.
  - A copy only-not the sole instance of the data.
- Personal information should always be transmitted in a securely encrypted format and never by email.
- Portable devices and storage media with personal information should be destroyed or erased so that there is no possibility of subsequent data recovery.

General Guidelines

Due to the inherent risks involving mobile devices, these should always be considered insecure and therefore require protection according to the following guidelines.

1. **Electronic Records/Mobile Device:** To the greatest extent possible, personal information should not be stored on or accessed from mobile devices. This simple rule does much to reduce risk.
2. **Data Encryption:** If personal information must reside on a mobile device, it should be encrypted. The decryption key should be entered manually; this step should not be automated. A means should exist to recover encrypted data when the decryption key is lost. Whole-disk encryption is potentially the most secure option

available. Since encryption standards are always evolving, school boards/authorities are responsible for ensuring that any solution selected meets the generally accepted standards in effect at the time. Encryption installations need to be regularly reviewed and updated as necessary. If in doubt, please refer to your Information Technology Team for support.

3. **Multiple Copies of Data:** Personal information residing on mobile devices should not be the only copy. Make sure there is another copy on a more secure device such as a server that is backed up regularly.

4. **Data Destruction:** The normal process for deleting data from a hard drive, USB flash drive, cell phone memory, etc., does not completely delete the data. Tools are readily available to easily recover deleted data and even fragments of files from these devices. Even if data is encrypted, it has to be decrypted for use and may therefore exist unknowingly in decrypted form in a temporary file that can be recovered even after deletion. Consequently, sensitive data should be destroyed or erased so there is no possibility of subsequent data recovery. Mobile devices and other electronic equipment that contain or access personal or confidential information, or have been used to access sensitive information in the past, should be processed to ensure all data is permanently removed in a manner that prevents recovery before these devices are redistributed to another employee, disposed of as surplus equipment, or returned to the vendor.

5. **Password Protection:** Access to the mobile device should be protected by the use of a strong password. Please refer to the PIM taskforce password guideline for strong password. On mobile devices, do not automate the supplying of passwords or other security credentials needed to access sensitive data (for example, automatically authenticating to an application or database that contains sensitive information, or having Microsoft Windows store passwords to these systems).

6. **Password Storage:** User IDs and passwords permitting access to the mobile device should never be stored in "plain text" (i.e., unencrypted so they can be easily read) on mobile devices.

7. **Physical Protection:** Reasonable care should be taken when using mobile devices in public places, meeting rooms, or other unprotected areas to avoid unauthorized access to or disclosure of the information stored on or accessed by the device.

   Special care should be taken in crowds, meetings, and security-screening areas to maintain control over the device. Do not let it out of your sight.

   - Mobile devices should not be left unattended and, where possible, should be physically locked away or secured. Use a cable lock with an audible alarm when not working on them,
   - Mobile devices should be transported as carry-on luggage whenever travelling by commercial carrier unless the carrier requires otherwise.
   - Do not leave mobile devices containing personal information in your vehicle. (If it absolutely cannot be avoided, lock them in your trunk before you start the trip, not in the parking lot of your destination or in other places where you can be publicly observed. If the vehicle does not have a trunk, leaving the device in the vehicle is not a secure option.)
   - All mobile devices should be discreetly and permanently marked as school board/authority property and should indicate a method of return in case the device is lost.
   - Enable the automatic lock feature of your device after five minutes or more of idle time.

- Conduct confidential work only on mobile devices over which you have control. Do not use public computers or networks or work on personal or confidential material in public places, and do not perform this type of work on computers that are shared with family members.
- While viewing personal information on a mobile device screen at locations outside the office, ensure that the screen cannot be seen by anyone else. Personal information should never be viewed on a mobile device screen while in the public.
- Software tracking and protection should be employed wherever possible. This may take the form of an inventory system to track the devices and/or a centrally administered software solution that can force passwords and security policies for mobile devices.

8. **Virus Protection:** Any mobile device capable of using antivirus software and anti-spyware programs should have the software installed and configured to provide real-time protection. The programs must be updated regularly with the latest security patches.

9. **Cell Telephones:** When in transit or working outside the office, employees should avoid using cell phones to discuss personal information. Cell phone conversations can be easily overheard or intercepted by individuals using scanners or other devices.

10. **Training Related to Mobile Devices:** Employees should be trained on the proper usage of the mobile device. Training should include privacy and security requirements as well as responsibilities for appropriate care of information according to these general guidelines.

11. **Loss or Theft of Mobile Device:** A privacy breach occurs when personal information is collected, retained, used, or disclosed in ways that are not in accordance with the provisions of the *Municipal Freedom of Information and Protection of Privacy Act*. Among the most common breaches of personal privacy is the unauthorized disclosure of personal information, contrary to section 32 of the Act. For example, personal information may be lost, stolen (especially from laptop computers, a prime example), or inadvertently disclosed through human error, and upon learning of a privacy breach, immediate action should be taken. Users should contact their FOI Coordinator immediately or refer to their Board's Privacy Breach Procedure.

References

Kansas State University, Information and Privacy Commissioner Office

PURPOSE

This guideline reflects best practices for securing personal information when working outside of the office or school. When working away from the school or office, records may be removed from the office or created off-site. This raises concerns about the privacy and confidentiality of records.

Overview

When personal information is in the care and/or custody of school board/authority employees they are responsible for ensuring that the information is protected and privacy is not breached.

This applies to records and information in all formats (paper, computer, photos, drawings, recordings, etc.).

Employees working off-site often convey information and records through various means including technology. In particular, technology has a significant impact on how records are handled and on how personal and other information is collected, stored, and communicated.

While this technology is efficient, it may diminish the confidentiality of the information transmitted. For that reason, the Information Privacy Commissioner suggests that institutions encourage employees take special care when using technology.

Guidelines

Refer to the following guides found within the toolkit for more detail:

1. Guidelines for Password Procedures
2. Guidelines for the Securing Mobile Devices
3. Technical Guidelines for Data Encryption
4. Considerations for the Use of Electronic Records in Place of Paper
5. Information Technology Equipment Hardware Disposal and Redistribution Guidelines
6. Privacy Breach Protocol

Recommendations

- Mobile technologies used outside the office include laptop computers, jump drives, cell phones and PDAs. Any technology that has sensitive information stored on them must be secure at all times.
- Sensitive information should not be stored on mobile devices if possible.
- Sensitive information, if stored on mobile devices, should be:
  - securely encrypted
  - a copy — not the only instance of the data
- Sensitive information should always be transmitted in a securely encrypted format and never by email.
- Portable devices and storage media with sensitive information should be destroyed or erased so there is no possibility of subsequent data recovery.
- Original records with sensitive information should not be removed from the work site.

Considerations for protecting records when working offsite

- Whenever practical, the original should remain on-site and only copies removed. Copies should be clearly identified as such and shredded when no longer needed.
- Utilize a sign-in/sign-out procedure with a due-back date to monitor removed files. Whenever possible, remove only relevant documents or an extract or summary.
- Return records to a secure environment as quickly as possible, for example, at the end of a meeting, the end of the day, or the end of a trip.
- Retain all working copies according to your institution's records retention schedule, or disposed of in a secure manner so that the record may not be reassembled and read.
- Records containing personal or confidential information should never be discarded in a client's or a public trash or recycling bin.
- Records should not be left unattended and, where possible, should be physically locked away or secured.
- Records in any format should be transported as carry-on luggage whenever travelling by commercial carrier unless the carrier requires otherwise.
- Do not leave paper records or mobile devices containing personal information in your vehicle. (If it absolutely cannot be avoided, lock them in your trunk before you start the trip, not in the parking lot of your destination or other visible location. If the vehicle does not have a trunk, leaving the device in the vehicle is not a secure option.)
- All paper records and mobile devices should be discreetly and permanently marked as school board/authority property and indicate a method of return in case the device is lost.
- While viewing personal information at locations outside the office, ensure that it cannot be seen by anyone else.

Working from Home

Designate a secure work area as "office space."

If possible, and where appropriate, install a second telephone line dedicated to work-related calls. This is particularly important for employees who need a phone line for a fax or modem. If an answering machine or answering service is required, ensure work-related messages can be accessed only by the employee. It is advisable to have a machine separate from that of the household or to use a password different from the household's to access work-related messages from an answering service.

Employees should store all paper and electronic records in the most secure fashion available.

Cell Telephones

Avoid using cell phones to discuss personal information. Cell phone conversations can be easily overheard or intercepted by individuals using scanners or other devices.

When making telephone calls from outside the office, employees should safeguard personal and confidential information as much as possible. For example, consider the physical setting to ensure that no one overhears a telephone conversation.

References

Kansas Sate University, Information and Privacy Commissioner Office

PURPOSE

This guideline outlines the privacy, copyright, and environmental considerations that should be addressed by school boards/authorities when redistributing or disposing of computer systems and electronic storage media. Specifically this guideline recommends process for the removal of personal information from equipment, the appropriate use of software licenses and consideration of the disposal of equipment in an environmentally and socially responsible manner.

All school board/authority computer systems, electronic devices and electronic storage media should be cleaned of sensitive personal or confidential data when no longer needed or before reuse to ensure the continued protection of personal and corporate privacy.

The school board/authority must dispose of all technology hardware and software in accordance with legislation, including but not limited to regulating waste and respecting copyright and licensed software.

School boards/authorities should have a hardware disposal and redistribution procedure in place to promote the secure disposal and redistribution of information technology hardware and electronic storage media. This document includes a number of best practices for developing a procedure.

Definitions

Electromagnetic Degaussing is a method of erasing or destroying data stored in magnetic media, such as hard drives, floppy disks, and magnetic tape using a strong magnetic field.

Electronic Storage Media is defined as any device that is used to store or record electronic information, including, but not limited to hard disks, magnetic tapes, compact disks, videotapes, audiotapes, handheld electronic devices, and removable storage devices such as floppy disks and zip disks.

Overwriting is one method of sanitation and is used to replace previously stored data on the electronic media with a pattern of meaningless random or non-random information.

The RCMP Technical Security Standard for Information Technology (**TSSIT**) specifies security standards for information technology including media sanitization requirements. Media may be sanitized by using a software application that overwrites the media a minimum of three times by using a degausser or by physically destroying the media.

Sanitizing is defined as the removal of information from electronic media or equipment such that data recovery using standard techniques or analysis is prevented.

Background

A large volume of electronic data is stored on computer systems and electronic storage media throughout the school board/authority. Much of this data consists of sensitive personal or confidential information, including student records, financial data, and personnel records. The school board/authority is covered by legislation that sets forth responsibilities for protecting this information including the *Education Act,* the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), and the *Personal Health Information Protection Act* (PHIPA). In addition, copyright laws and software license agreements protect vendor rights regarding the use of software. Much of the software used by the school board/authority is licensed under special academic licensing agreements which prohibit the transfer of this software outside the school board/authority.

Unauthorized disclosure of sensitive information may subject the school board/authority to legal liability, negative publicity, and monetary penalties. All sensitive information and licensed software must be properly removed when disposing of computer systems with hard drives, PDAs, removable media, and other electronic devices capable of storing information.

Simply deleting files from the media or formatting a hard drive is not sufficient to completely erase data so that it cannot be recovered. In order to prevent deleted information from being recovered the school board/authority needs to overwrite all previous stored data or to destroy the media by physical force or electromagnetic degaussing.

Scope

This guideline applies to all workstation and storage media hardware purchased, owned, controlled or used by the school board/authority, including equipment purchased by the school board/authority on behalf of individuals or departments within the school board/authority, donated equipment, and equipment in any other way obtained and owned by the school board/authority.

Guidelines

- Equipment that is no longer required may be redistributed within the school board/authority, sold, salvaged for parts, donated to an appropriate charitable organization, or disposed of. Equipment that does not meet the school board's/authority's minimum standard for computer equipment and thus cannot be redistributed within the school board/authority is often of little value to sell or donate and generally should be salvaged for parts or securely disposed of.
- All data (including encrypted data) should by default be considered potentially personal or confidential and should be subject to these procedures.
- Once obtained for school board/authority use, all technology hardware and software should be documented and tracked for inventory control in accordance with school board/authority guidelines. All equipment and software should be tracked centrally from point-of-purchase to disposal.
- The proper disposal and redistribution of school board/authority information technology equipment should be coordinated by a centralized department. A method of disposal inventory should be maintained to ensure, on behalf of the school board/authority, that the liability for technology hardware and software has been relinquished.

- Any equipment which is donated, parted, or disposed of, should have a completed disposal record form with description, serial number, date discarded, method of disposal, and purchase value, if any.
- School board/authority-owned electronic devices and computer systems should be sanitized prior to removal from the school board/authority. This includes removing all school board/authority data and licensed software from the equipment.
- Personal and confidential data should be removed from hardware before it is made available for reuse, even within a department or elsewhere within the school board/authority.
- School board/authority-leased computer systems should be sanitized as part of the end-of-lease processing.
- Erasure tools used in the sanitization process should meet RCMP standards and be approved by the school board/authority. Staff members should take reasonable steps to ensure that these tools are used properly.
- Departments and schools should relinquish all obsolete, broken, or unwanted technology items to a designated department for disposal.
- Removable storage media should not be passed on with equipment but instead should be securely erased, retained by the department, or disposed of by secure means.
- Storage media used to store electronic personal or confidential information should not be released outside of the school board/authority for any reason. This includes vendor or manufacturer service, maintenance, repair, or replacement of the device or the host workstation or server, until such time as it has been cleaned of any personal or confidential data or information unless strict contractual obligations have been imposed. Whenever possible equipment repair should be done on-site.
- Non-rewritable electronic media containing personal or confidential information should be physically destroyed when no longer used or no longer needed.
- Rewritable electronic media containing personal or confidential information should be erased in such a way that the data or information on the device cannot be recovered or the media should be physically destroyed.
- A school board/authority employee, who generates, copies, or records electronic personal or confidential information on local or removable media is responsible to safeguard the confidentiality and ensure the integrity of that electronic personal of confidential information. The employee should ensure that proper procedures are followed for any removable storage devices to be disposed of or reused.
- All equipment should be discarded in an environmentally and socially responsible manner. Any disposal of computer systems and media must comply with all environmental regulations. Some electronic equipment is classified as toxic waste and needs to be disposed of accordingly. Whenever possible, electronic equipment should be recycled by an accredited recycling company.
- The destruction of data and software may be handled by a recycling company if there are strict contractual obligations in existence to ensure the destruction of the data and the protection of personal and confidential information.
- This policy, associated forms, and a list of approved disk sanitation software should be published on the school board's/authority's website.

Auditing and Evaluating Hardware Disposal and Redistribution

The school board/authority should ensure that hardware disposal and redistribution procedures are subject to regular audits. These audits should address the school board's/authority's compliance with the operational policies, guidelines and procedures. An external body may be retained in order to perform the audit. The school board/authority should endeavour to immediately address any deficiencies or concerns identified by the audit.

The school board/authority should regularly review and evaluate its hardware disposal and redistribution procedures and related procedures and guidelines to determine if they comply with current legislation and are appropriate given current technology. In the event that significant related legislative changes occur, the policy should be reviewed and updated as needed.

References:

Royal Canadian Mounted Police, *Technical Security Standard for Information Technology* (TSSIT), August 1997.

Royal Canadian Mounted Police, *Hard Drive Secure Information Removal and Destruction Guidelines,* October 2003.

Sources

1. Bristol University - Information Services - *Disposal of computer equipment: University policy*
2. Clark County, Washington - *Information Services Equipment Disposal Policy*
3. Eckerd College - *Computer Equipment Disposal Policy*
4. University of Physician and Surgeons - *Workstation and Storage Media Hardware Disposal and Re-Use*

PURPOSE

The purpose of this document is to outline the procedures and guidelines to be used when students, teachers and other school board/authority employees publish material on the Internet using the school board/authority or school website(s). This document focuses on privacy and security issues. School boards/authorities should develop a more complete policy or guideline on the use of websites within their school board/authority in order to make effective use of the technology.

Background

Schools and school boards/authorities need to have policies and procedures which include; what types of information will be posted to the website; who will be responsible for determining the information to be posted; a procedure for obtaining consents and who will be responsible for responding to any complaints that may arise. In addition, schools, and school boards/authorities should post their privacy policies on their websites.

The school board/authority should provide a web-based infrastructure to schools and to teachers to augment learning through the use of the Internet.

Schools have been using print material, such as newsletters, to communicate education-related information to parents/guardians and students. Many schools are using the Internet to disseminate information to parents/guardians, students, and the community at large. The use of the Internet is widespread and as such, challenges people to think about access and privacy in a professional capacity as well as personally. While it offers access to information at an unprecedented level and speed, the Internet can also threaten the privacy of staff and students as never before. It is critical that the school board/authority be aware of these challenges and provide guidelines to its employees in order to maximize the benefits of the Internet and minimize any loss of privacy to staff and students.

All school board/authority programs, schools, and departments are encouraged to contribute relevant content to the school board's/authority's website. The web provides an excellent communication tool to reach the school board's/authority's many audiences. School boards/authorities may maintain more than one website; generally one aimed at the community, students, parents, and vendors; and another internal websites (portal) for content directed to staff. As with any communication tool, it is essential for the school board/authority to project a professional image. It is critical that the school board/authority website is user friendly and easy to navigate, maintaining visual standards, content accuracy, currency and relevancy, and technical accuracy.

As schools are familiar with the Internet and its many uses, they are creating their own school websites, to establish their presence on the web. Websites make information about the school available to the school community as well as to the public worldwide. Such websites are an excellent means to inform viewers about the school. Visitors from around the world will view school websites. It is important that all school websites reflect the board goals, maintaining respect for copyright and intellectual property. To that end, these guidelines are being put in place, to ensure that the information contained on school websites is accurate and appropriate for the school or school board/authority and to protect personal information.

Definition

A web page can consist of text, pictures, video and/or sounds. Web pages are found on the internet and are displayed on a computer monitor. Web pages can contain any information that is placed onto it by the author. Web pages can be accessed via the internet and thus the world has access to the information. Every web page is identified by a unique web address or URL (Uniform Resource Locator). These can be created using HTML (hypertext markup language), DHTML (Dynamic HTML) and JavaScript and are translated by a Web browser. A web page is an individual HTML document and a website is a collection of pages. The first webpage usually requested at a website is called the "home page."

Disclosure of Personal Information

Personal information by the definition provided by the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) is, in essence, "any information about an identifiable individual or rendering an individual identifiable." An image of students' work that has their name attached and contains identifying information is an example of personal information, Personal information is subject to the application of certain laws pertaining to its collection, use, and disclosure.

Notice alone may be sufficient when:

- Collection is for internal use only; when the information remains in the school board's/authority's custody.
- Use and or disclosure remains under the school board's/authority's control for example when a legal agreement is established such as with external school photographers.
- Disclosure is considered reasonable and expected - fits within the definition of the provision of educational programs, e.g., student displays.

Signed consent is required when:

- Disclosure takes the information out of the school board's/authority's control, e.g, over the Internet.
- The intended use or disclosure is not within the definition of the provision of educational programs and could be viewed as possessing the possibility of breaching an individual's personal privacy.

Notice and signed consent should:

- Cite legal authority (e.g., Education Act, Municipal Freedom of Information and Protection of Privacy Act).
- Explain the purpose(s) for the information.
- Provide contact information of an employee responsible for the activity.
- Provide opportunity to opt out of participating.

Notice:

- Notice and opportunity for signed consent should occur well in advance of the activity. In addition, notice can be posted on the school website.
- There may be occasion when notice of collection is not required (e.g., where the collection is for the purpose of determining eligibility for an award). Each instance must be evaluated on its own merit.

Website Publications:

- School administrators must ensure that Internet permission forms are completed before any personal information is posted or published on a school website or the school board/authority website.

Use and Disclosure:

- When appropriate collection rules have been satisfied, information can be used and/or disclosed as described in the notice of collection.
- If the use or disclosure changes from that described in the notice of collection a subsequent notice or informed consent must be provided/sought.
- Each individual retains a right of access to their own information with very few exceptions.

Retention:

- All web pages and personal information must be retained for a minimum of one year (12 months) from the date of last use unless:
  - as otherwise set out in the school board's/authority's retention schedule or resolution;
  - its regulation requires a longer retention period;
  - the individual to whom the information relates consents to its earlier disposal.

Recommendations

- Avoid using images of actual students and staff wherever possible. Use instead:
  - stock images (found on the Internet for example);
  - images of things as opposed to persons (e.g., schools);
  - animation;
  - blurred or distanced images.

Reference to Guidelines on Privacy Act Notification Statement

Personal Information

Schools hold many different types of personal information. Due to the nature of certain types of personal information, some information should never be included on any websites. This would include:

- Student's report card and academic transcript/individual student marks
- Student's Ontario Student Record (OSR)/Ontario Education Number
- Student's telephone number, home address, personal email address
- Parent's telephone number, home address, personal email address
- School and/or school board/authority staff's home address, telephone number, personal email address

Some students may not be concerned about their personal information being posted on the school website, and hence the web, while others are apprehensive. Types of personal information, which school board's/authority's may decide to post, provided the proper consent is obtained, in advance, include:

- Photographs of students (individual and/or group)(with or without a name)
- Students' work (e.g., essays, projects, etc., with or without a name)
- Names of students participating in extracurricular activities and student council
- Names of students award-winners/prize/scholarship winners
- School yearbooks (names and photographs)

Some information may be considered "non-personal" when used alone but, when combined with a second piece of information, becomes personally identifying. A picture or a name on its own may not be considered "personal information," but together will form an identity that can be recognized.

Information that may be personal information, depending on its content

It should be noted that certain types of information may not appear to be personal information, but depending on the content, may contain personal information.

Examples of types of information, which may contain personal information are:

- School newsletters
- Minutes of meetings, including those of school councils
- Information on school events, such as fundraisers, drama productions, athletic competitions, science fairs

The above records need to be reviewed on a page-by-page basis. If they contain personal information, they should only be posted to the website if the personal information is edited out, or if the individuals to whom the personal information relates have consented to its posting.

Intranet and Collaborative Spaces

An intranet is a network of computer servers that hold and share information owned by the school board/authority that are accessible only by authorized users. School boards/authorities should develop and publish intranet access and use guidelines, available to staff and/or students internally. Guidelines should outline the purposes, benefits, and risks associated with the use of intranet resources. The school board/authority is responsible for facilitating the setup, maintenance, and monitoring of user accounts to the intranet.

Collaborative spaces (including forums) blogs and wikis may also be available for staff and/or students internally. These collaborative spaces are not intended for finalized school board/authority information. Collaborative spaces are areas for collaboration and may refer (link) to documents on the school board's/authority's official website(s), such as minutes of meetings or calendars for specific initiatives. The school board/authority should provide a means for users to report any inappropriate communication such as attempts to engage students in contact outside of the school.

Guidelines for School Websites

The principal is responsible for the content of the school website. Any school creating a website should have a webmaster appointed by the principal. The webmaster should assist the principal in ensuring that these guidelines are adhered to and that the content of the school web pages meets the principal's approval.

- For consistency, maintainability, URL management, site security, and other related issues, all organizations of the school board/authority, including schools must host their sites on the school board/authority web server.
- The content of the school website and associated links must be consistent with the educational aims of the school board/authority.
- School web pages should not contain any commercial or promotional advertising. School web pages may contain small acknowledgements of school partnerships or sponsorships, which are in accordance with the written approval of the Director.
- All school websites must contain a link back to the school board/authority home page. This link must be prominent and displayed on the school's main page.
- No school page content should provide the means for people to contact any student directly. If communication back to the school is needed, it should be directed to the appropriate staff member.
- Pictures of students included on school web pages must NOT include student names. Similarly, schools should not use filenames for pages and images which include student names. First names can be used for samples of student work.
- When using pictures of persons on the school website, the school should obtain written permission.
- Personal home pages for students or staff members are not permitted.
- School web pages must not use copyrighted materials without permission.
- The principal must be clearly identified on the main page with the principal's email address prominently displayed. All correspondence to the site should go to the school identified school website contact. Where a teacher has a curriculum project that requires email responses, the principal can authorize the listing of the teacher's email address and not receive copies of the responses.

- The date of the last update must be clearly identified on the main page.
- To encourage currency of school pages, it is recommended that each school web page on the school board/authority site be disabled if the date on the school main page is more than six months old and information is out of date. Schools should be contacted prior to disabling the page.

Principal's Guidelines for Selecting a School Webmaster

The school webmaster should be a staff member who can facilitate or develop the ability to do the following if required for the school's website (system support will be available):

- Use a web editor
- Create and edit .gif and .jpg pictures
- Create transparent gifs
- Use HTML (basic fluency)
- Use the generally accepted principles of good web page design
- Assess strengths and weaknesses of current web implementation

The school webmaster should:

- In cooperation with the school principal, know and apply the school board's/authority's policy in relation to the school's website.
- Be responsible for ensuring that the school's website is posted to the board's server.
- Ensure the school's website is updated at least every four months or inform the school board's/authority's webmaster that an update is not needed.
- Coordinate the following:
- Quality control of content and design of the school's website
- Incorporation of new ideas and technologies into the site as the resources become available
- Periodic check of links to ensure they are current and still meet the school board's/authority's website guidelines and, if needed, make appropriate changes
- Identification of website bugs and problems and development of strategies to correct these problems.

Guidelines for Teacher Websites

A teacher website, under the direction of the principal, should be self-administered.

A teacher website should be directly related to the classroom curriculum.

Examples of classroom curriculum-related/educational material(s) are:

- Assignments
- Upcoming events or trips - being careful that posting time and place information may have impact on issues of custody.

- Sample lessons
- Board-recommended educational sites
- Board-recommended curriculum projects

Examples of non-classroom curriculum material, and therefore not permitted for posting, are:

- Individual student marks
- Attendance
- Personal information (non-classroom-related)
- Links to commercial websites
- Communicating to parent(s)/guardian(s)/student(s) by electronic means.

As a general principle, the teacher should not post personal information on his/her website. However, if the school board/authority-recommended educational sites or the school board/authority-recommended curriculum projects require the posting of students' personal information, then the teacher should obtain informed consent from all affected individuals or from a person who is authorized to consent on their behalf.

Informed consent **requires that the person consenting understand the exact nature of the information for which consent is sought, understand the potential consequences of signing the consent form, and be given the right to revoke the consent at any time. Students 16 or older must sign the consent form.**

The teacher should be responsible for the timely updating and removal of outdated information on his/her server space. As well, the teacher should be responsible for the ongoing quality and relevancy of the information on the teacher's website.

The home page should contain the full name and mailing address of the school and a date of creation/update. There should be a visible statement/logo that this site is part of the school board/authority with a link back to the school board/authority home page.

Any concerns or questions about the site should be referred to the principal.

The Copyright Act (Canada) must be respected. It is the responsibility of the employee to understand the rules for reproducing a copyright-protected work.

Student Web Pages

Students may create a website as part of a class activity.

- Material presented on a student class activity website must meet the educational objectives of the class activity and be approved by the teacher and the school principal.
- Student web pages must include the following notice: "This is a student web page. Opinions expressed on this page are those of the student and may not necessarily reflect the opinions of the school or school board." This notice should be in bold print.
- It is not considered a violation of a student's rights to free speech to require removal of material that fails to meet established educational objectives or that is in violation of a provision of the school board's/authority's Acceptable Use Guidelines or student disciplinary code.

General Information/Personal Information: Individuals' Professional Responsibilities/Professional Capacity

Reference MFIPPA section 2.1

Information encountered in the course of one's professional capacity or individual professional responsibilities, does not constitute "personal information" as cited in MFIPPA legislation, Section 2.1. Examples of this type of information are:

- Staff lists with staff members' names, titles, contact information, department, and grade taught
- Names of staff members responsible for extracurricular activities
- Names of volunteers/community members/schools
- Photographs of staff members (individual and/or group photos)
- Photographs of volunteers/community members (individual and/or group photos)

Although there are no privacy provisions under MFIPPA legislation that must be considered in this category, other issues may arise. Consent should be obtained from each staff, volunteer, and community member prior to posting their general or personal information on the web.

Accessibility

The Web is an increasingly important resource in many aspects of life for staff and students. School board/authority and school websites should be accessible in order to provide equal access and equal opportunity to staff and students with disabilities to more actively participate in the school board's/authority's education goals. Web accessibility encompasses all disabilities that affect access to the Web, including visual, auditory, physical, speech, cognitive, and neurological disabilities.

Web accessibility though various technologies offers the possibility of access to information and interaction and to overcome barriers inherent in print, audio, and visual media.

References

1. The Information and Privacy Commissioner/Ontario, Upper Grand District School Board and Peterborough, Victoria, Northumberland and Clarington Catholic District School Board - *Posting Information on Websites: Best Practices for Schools and School Boards*
2. Grand Erie District School Board - *Web Publishing Guidelines*
3. London District Catholic School Board - *Guideline for School Websites*
4. London District Catholic School Board - *Website Terms of Use*
5. York Region District School Board - *Website Disclosure and MFIPPA*
6. York Region District School Board - *Web Standards*
7. The Dufferin-Peel Catholic District School Board - *Posting Information on the Internet as it Applies to the World Wide Web - By Schools and Teachers AND Consent Forms*
8. Simcoe County District School Board - *Acceptable Use of Tech Guidelines - Draft*
9. Halifax Regional School Board - *Draft Acceptable Use of Computers and Internet/Intranet Technology Policy*
10. Web Accessibility Initiative - "*Introduction to Web Accessibility*" (www.w3.org)

Appendix

Sample Website Terms of Use

Sample Website Privacy Policy

Sample Website External Links Disclaimer

Sample Website Copyright Protection

Consent Forms

Sample Website Terms of Use

A website is maintained by a school or school board as a public service to students, parents, staff, and site visitors from the community and beyond. The board cannot guarantee that all information is current or accurate. Website users should verify all information before acting on it. The school board reserves the right to change or modify its terms, conditions, and notices under which use of the website is offered. Continued use of this website constitutes an agreement to all such terms, conditions, and notices. Communications made through this website's email and messaging system should in no way be deemed to constitute legal notice to the school board or any of its agencies, officers, employees, agents, or representatives, with respect to any existing or potential complaint, grievance, claim, or cause of action against the school board or any of its agencies, officers, employees, agents, or representatives.

Sample Website Privacy Policy

The school board respects the privacy of its Web visitors. Personal information on the Internet is protected in the same way it is protected in all other ways that are communicated and interacted with. Staff should adhere to strict policies that protect the confidentiality of any personal identifiable information such as names, email addresses and telephone numbers. The use of cookies is strictly prohibited except to provide data on a performance measure of meeting informational or service needs relative to the Internet site. The only personal identifying information collected from use of the school board website is from submitting comments, suggestions, or questions through a feedback form or an email. The school board will not sell, rent, or release personal information to third parties.

Sample Website External Links Disclaimer

There may be websites linked to and from this site that are operated or created by or for outside organizations. Those organizations are solely responsible for the operation and information (including the right to display such information) found on their respective websites. The linking to or from this site does not imply on the part of the school board or any of its employees any endorsement or guarantee of any of the organizations or information (including the right to display such information) found on their respective websites. The school board does not assume and is not responsible for any liability whatsoever for the linking of any of these linked websites, the operation or content (including the right to display such information) of any of the linked websites, nor any of the information, interpretation, comments, or opinions expressed in any of the linked websites. Any comments or inquiries regarding the linked websites are to be directed to the particular organization for whom the website is being operated. The board reserves the right to block access to and from inappropriate Internet domains, email addresses, or websites.

Sample Website Copyright Protection

Materials on this website were produced and/or compiled by the School Board to provide visitors with direct access to information about the programs and services offered by the School Board. The material on this website is covered by the provisions of the Copyright Act and all applicable federal and provincial statutes. Such provisions serve to identify the information source and, in specific instances, to prohibit reproduction of materials without written permission. Any reproduction or commercial use of the materials is strictly prohibited without written permission of the School Board. To obtain information concerning copyright ownership and restrictions on reproduction of materials on this site, please contact the School Board webmaster.

Consent Forms

In order to ensure that all staff use board and school websites properly, with respect to posting personal information, they are required to obtain consent from all affected individuals or from a person who is authorized to consent on their behalf.

This should be a one-time requirement for each school year and for each school. If a staff or student moves to a new school, a new consent form should be obtained. (Note: Such consent must also be reaffirmed if the nature of the posting is different than that generally described in the original consent form.)

Informed consent requires that the person consenting understand the exact nature of the information for which consent is sought, understand the potential consequences of signing the consent form, and be given the right to revoke the consent at any time.

Only persons having lawful custody of the student may sign this consent form as parent or guardian. In cases of joint custody, it is advised that both parents provide consent.

For those situations where an individual whose consent is required is mentally incapable and a substitute decision maker has been appointed under Ontario Law to act on his/her behalf, then the individual appointed as substitute decision maker should sign the consent form.

CONSENT FORM
For Posting Student's Personal Information on a School's Website

This consent form meets the requirements of the *Municipal Freedom of Information and Protection of Privacy Act* and the *Education Act* for the disclosure of personal information. It provides for consent that is both informed and voluntary, and relates to clearly identified information to be used and disclosed for clearly defined purposes.

By signing this document, I/we consent to the disclosure of personal information about _____ (name of student)

by posting it to the website of _____ (name of school) and hence to the World Wide Web.

This consent only applies to the items below that I/we have initialed:

_____ Photograph of _____ (name of student)

_____ Group and class photographs including _____ (name of student)

_____ Essays written by _____ (name of student)

_____ Projects done by _____ (name of student)

_____ Awards, scholarships, prizes received by _____ (name of student)

_____ Participating of _____ (name of student) in any extracurricular activities

_____ Other specific activity identified by school (please specify) _____

I/we have read and understand the school board's policy on school websites. I/we are aware that by giving this consent,

I/we are permitting personal information about _____ (name of student)

to be posted to the _____ (school's website)
and hence to the World Wide Web, and that if consent were withheld, this posting would not occur.

I/We further understand that this consent is valid for one year and may be withdrawn by me/us at any time, upon written notice. In the event that consent is withdrawn, I/we understand that the information about me will be removed from the schools website, but understand that, in some cases, it is impossible to remove all traces of personal information from the Internet.

I/we have given this consent voluntarily: _____ (Date) on _____ (Place of signature; e.g., city)

For students under 16 years of age: _____
Signature of Parent/Guardian

For students aged 16 or 17 during the school year – signature of both the student and parent/guardian:

_____ Signature of Student

_____ Signature of Parent/Guardian

For students 18 years of age or over – signature of student:

_____ Signature of Student

CONSENT FORM
For Posting Student's Personal Information On A Teacher's Website

This consent form meets the requirements of the Municipal Freedom of Information and Protection of Privacy Act and the Education Act for the disclosure of personal information. It provides for consent that is both informed and voluntary, and relates to clearly identified information to be used and disclosed for clearly defined purposes.

By signing this document, I/we consent to the disclosure of personal information about _____
(name of student)

by posting it to the website of _____ and hence to the World Wide Web.
(name of teacher)

This consent only applies to the items below that I/we have initialed:

_____ Videotaping/digital video of _____ (name of student)
individually or in a group, participating in the board-approved educational site:

_____ (name of site)

_____ Videotaping/digital video of _____ (name of student)
individually or in a group, participating in the board-approved curriculum project:

_____ _____

I/we have read and understood the school board's policy on school Websites. I/we are aware that by giving this consent,

I/we are permitting personal information about _____ (name of student)

to be posted to the _____ (teacher's website)
and hence, to the World Wide Web, and that if consent were withheld, this posting would not occur.

I/We further understand that this consent is valid for one year and may be withdrawn by me/us at any time, upon written notice. In the event that consent is withdrawn, I/we understand that the information about me will be removed from the teacher's website, but understand that, in some cases, it is impossible to remove all traces of personal information from the Internet.

I/we have given this consent voluntarily: _____ on _____
(Date) (Place of signature; e.g., city)

For students under 16 years of age: _____
Signature of Parent/Guardian

For students aged 16 or 17 during the school year – signature of both the student and parent/guardian:

_____ _____
Signature of Student Signature of Parent/Guardian

For students 18 years of age or over – signature of student:

_____
Signature of Student

CONSENT FORM
For Posting Volunteer/Community Member Personal Information On A School's Website

This consent form meets the requirements of the Municipal Freedom of Information and Protection of Privacy Act for the disclosure of personal information. It provides for consent that is both informed and voluntary, and relates to clearly identified information to be used and disclosed for clearly defined purposes.

By signing this document, I consent to the disclosure of personal information about me,

_____ (name)

by posting it to the website of _____ (name of school)
and hence to the World Wide Web.

This consent only applies to the items below that I have identified with my initials:

_____ My photograph/image alone or in a group

_____ Extra-curricular activities I have supervised

_____ Projects and/or activities at the school that I have participated in/supervised/organized

_____ Profile of my work as a volunteer/community member

_____ Other specific activity identified by school (please specify) _____

I have read and understood the school board's policy on school websites. I am aware that by giving this consent, I am permitting personal information about me to be posted to the _____ (school's website) and hence to the World Wide Web, and that if consent were withheld, this posting would not occur.

I further understand that this consent is valid for one year and may be withdrawn by me at any time, upon written notice. In the event that consent is withdrawn, I understand that the information about me will be removed from the School's Website, but understand that, in some cases, it is impossible to remove all traces of personal information from the Internet.

I have given this consent voluntarily.

_____ _____
(Place of signature; e.g., city) (Date)

_____ _____
Signature of Volunteer/Community Member Printed Name

PURPOSE

The purpose of this document is to outline the procedures and guidelines to be used for school board/authority employees who maintain and/or transfer personal and confidential information using electronic means. This guideline is provided to assure the confidentiality and integrity of personal information should data encryption be used as an information protection control. This document is intended to provide guidance in understanding encryption technologies. It applies to all devices, physical or virtual where board data is stored. School boards/authorities may use this guideline in the development of policies or procedures for the use of data encryption within their school board/authority.

Definition

Encryption is a secure process for keeping personal and confidential information private. It is a process by which bits of data are mathematically jumbled using a password key. The encryption process makes the data unreadable unless or until decrypted.

Background

Data encryption can be an effective information protection control when managing staff or student personal data. School board/authority employees should understand that data encryption is not a substitute for other information protection controls such as access control, authentication, or authorization; that data encryption should be used in conjunction with those other controls; and that data encryption implementations should be proportional to the protection needs of the data.

Encryption Applicability

Transmission: Any data classified as personal and private and having a required need for confidentiality and/or integrity should be transmitted via encrypted communication to ensure that it does not traverse the network or web in clear text.

Applications of encryption for data transmission include, but are not limited to, the following:

- **File Transfers** - Encryption transfers can be achieved via the use of an encrypted transmission protocol or network service (e.g., WinSCP, SFTP, etc.) or by transferring a file that has been encrypted prior to the transmission.
- **Email** - Confidential content transmitted in email messages should be encrypted prior to the transmission, presented via a secure web application, or encrypted in a secure message format given that email is exposed to the possibility of unauthorized access at a number of points throughout the delivery process.
- **Interactive Sessions** - Encryption of private data, including login passwords, transmitted during remote login sessions (e.g., Telnet and remote control software for PCs) should be provided through the use of secure applications or protocols.

- **Web-Based Applications** - Encryption of private data communicated between a user's browser and a web-based application should be provided through the use of secure protocols (e.g., HTTPS, TLS/SSL, etc.). The display of data should be limited to only what is required by the user's authorized use of the application.
- **Network Printer Communications** - Encryption of private data that is output to a printer connected to a network can be provided through the use of secure printing applications (e.g., JetDirect) or protocols (e.g., IPP) to prevent unauthorized network interception.
- **Remote File Services** - Encryption of private data transmitted by remote files services should be provided through the use of encrypted transmission protocols (e.g., IPSec, ISAKMP/IKE, SSL/TLS) to prevent unauthorized interception.
- **Database Access** - Encryption of private data transmitted between an application server and a database can be implemented to prevent unauthorized interception. Such encryption capabilities are generally provided as part of, or an option to, the database server software.
- **Application-to-Application Communications** - Encryption of private data transmitted between cooperating applications should be provided through the use of commonly available encrypted protocols (e.g., SOAP with HTTPS) to prevent unauthorized interception.
- **Virtual Private Network (VPN)** - A VPN connection offers an additional option to protecting private data transmitted via the network when other alternatives are not feasible. The use of VPNs should be carefully considered so that all security and networking issues are understood.

Storage: Any data classified as personal and private and having a required need for confidentiality and/or integrity should be stored encrypted in systems and/or databases and/or portable media.

Applications of encryption for data storage include, but are not limited to, the following;

- **Whole Disk Encryption** - Encryption of private data stored on portable computing devices (e.g., PDAs, tablet PCs, laptops, and smart phones), as well as storage media, (e.g., CDs, DVDs, and USB drives) should be provided through the use of a whole disk encryption tool or one that can at least be configured to encrypt all personal data.
- **File Encryption** - Encryption of private data should be provided to facilitate the secure transport of individual files over a network without transmission encryption or to off-line storage devices (e.g., CDs, DVDs, or USB drives.)
- **Database Storage** - Encryption of private data contained in a database server should be provided through the use of whole disk encryption or through features native to the database server software. Encryption capabilities native to database server software may allow for encryption of specific tables or columns of a database and may also be required to segregate access rights among multiple applications that utilize a single database server.
  - Staff who hold data should understand that database server encryption does not imply that data in the database server is encrypted when transmitted over a network. In general, the database server decrypts data before it is transmitted; therefore, encryption for data transmission should also be implemented for database servers processing private data.
  - Staff who hold data should consider a number of factors when making decisions on database server encryption (e.g., data classification, need for confidentiality, number of associated applications, system administration, performance, cost, and backup requirements).
- **Backup and Archiving** - Encryption of private data contained in backups and/or archive copies should be provided to prevent unauthorized access.

Additional Mitigating Factors: A combination of business practices and technology can reduce the risk of unauthorized data exposure, thereby reducing the specific need to implement data encryption.

Examples of such mitigating factors include, but are not limited to, the following;

- Firewall Restricting Capabilities
- Detailed Audit Logging
- Detailed Process Logging
- Intrusion Detection Capabilities
- Intrusion Prevention Capabilities
- Integrity Checking Capabilities
- Separation of Personal and Confidential Duties
- Physical Security Capabilities

Encryption Services

Symmetric algorithms should be used for encrypting private information. Symmetric encryption is cryptography in which the same key is used to both encrypt and decrypt the data. It requires a separate secure channel to exchange keys. The following are symmetric algorithms:

- AES (128-, 192-, or 256-bit)
- RC6 (256-bit)
- Blowfish (128- or 448-bit)
- Triple DES (112- or 168-bit)
- RC4-128
- IDEA-128
- CAST-128
- RC5 (128-bit only)
- SAFER (128-bit)

Asymmetric algorithms should be used for public key encryption of private data. Asymmetric encryption is cryptography in which a pair of keys is used to encrypt and decrypt a message. The sender of the message encrypts the message with the recipient's public key. The recipient then decrypts the message with his/her private key. The following are public key asymmetric algorithms:

- RSA (minimum 1024-bit)
- ECC (minimum 384-bit)

Digital Signatures should be used to associate a user or entity with a respective public key. A public key is the publicly available key of a signature key pair that is used to validate a digital signature and/or to encrypt confidential information. For digital signature purposes when private information is involved, the following encryption services should be used:

- RSA (minimum 1024-bit) with SHA-1
- DSA (minimum 1024-bit) with SHA-1
- ECDSA (minimum 384-bit) with SHA-1

Digital Certificates should apply recognized standards (e.g., X.509v3) and should, at least:

- Identify the issuing certificate authority - the certificate authority should be one authorized by records management or strictly designated for internal board usage;
- Identify the individual (subscriber) who is the subject or entity designee named or identified in a certificate issued to that individual and possesses a private key, which corresponds to the public key listed in the certificate;
- Provide the subscriber's public key ;
- Identify its operational period;
- Be digitally signed by the issuing certificate authority.

Encryption Key Management

1. Encryption keys used to protect personal data should also be considered personal data.
2. Professional key management is critical to prevent unauthorized disclosure of personal data or irretrievable loss of important data. A centralized school board/authority key management infrastructure should be made available to all school board/authority staff to ensure appropriate controls are applied. The school board/authority data managed by all key management infrastructures should be considered both personal and mission-critical.
3. All school board/authority key management infrastructures should create and implement an encryption key management plan to address the requirements of these encryption guidelines, other school board/authority policies, and applicable education and/or privacy law.
    - The encryption key management plan should ensure that data can be decrypted when access to data is necessary. Backup or other strategies (e.g., recovery agents, etc.) should be implemented to enable decryption; thereby ensuring data can be recovered in the event of loss or unavailability of encryption keys.
    - The encryption key management plan should address handling the compromise or suspected compromise of encryption keys. The plan should address what actions should be taken in the event of a compromise (e.g., with system software and hardware, private keys, or encrypted data).
    - The encryption key management plan should also address the destruction or revocation of encryption keys that are no longer in use (e.g., the user has left the school board/authority) or that are not associated with a key management program.

4. All symmetric encryption keys used on systems associated with personal data should be randomly generated according to industry standards. Acceptable standards include, but are not limited to, the following;
   - FIPS 186-2
   - ANSI X9.31
   - ANSI X9.62
   - ANSI X9.82
5. Where symmetric encryption is used to protect personal data:
   - Master keys (keys used to derive other symmetric keys) should be changed at least once per year.
   - Key-encrypting keys (keys used to encrypt other keys using symmetric key algorithms) should be changed at least twice per year.
   - Data-encrypting keys (keys used with symmetric key algorithms to apply confidentiality protection to information) should be changed once per session or every 24 hours.
6. When asymmetric encryption is used, the operational period of asymmetric keys associated with a public key certificate is defined by the encryption key management plan of the issuing certificate authority.
7. Encryption keys should be stored within an encrypted key store or an otherwise encrypted form using approved algorithms, or the keys may be stored on a security token (e.g., a smart card). The encryption keys should never leave the device if stored on a security token.
   - This requirement does not pertain to keys (e.g., SSH host keys) or protocols (e.g., encryption used by backup technologies) that are providing layers of encryption transport in addition to the strong encryption that has already been applied to personal data.
8. Encryption keys are confidential information, and access should be strictly limited to those who have a need to know. The owner(s) of data protected via encryption services should explicitly assign responsibility for the encryption key management that should be used to protect this data. If keys are transmitted over communication lines, they should be sent in encrypted form. The exchange of keys should employ encryption using a stronger algorithm than is used to encrypt data protected by the keys.
9. Encryption keys that are compromised (e.g., lost or stolen) should be reported immediately to the school board/authority office, the key manager, and the information owner of the data being protected. The key should be revoked or destroyed and a new key generated. Key re-assignments should require re-encryption of the data.

Certificate Authorities

1. Encryption keys that are generated by a certificate authority (CA) and used to control access to the CA server or used by the CA to perform functions should be stored on Hardware Security Modules (HSM).
2. All HSMs used within the school board/authority should adhere to recognized standards (e.g., FIPS 140-3).
3. School board/authority CAs must be designed such that all CA administrator functions are accounted for in detail. Ideally, no single administrator should obtain full access to the CA encryption keys (e.g., access measures should involve separation of duties, dual control, etc.)
4. School board/authority CAs within the school board/authority should adhere to an encryption key management plan.

References

University of Texas – *UT Austin Data Encryption Guidelines*
http://www.utexas.edu/its/policies/opsmanual/encrypt-guide.php

UT-Austin: IT Security Operations Manual

UT-Austin: Data Classification Standard

UT-Austin: Minimum Security Standards for Systems

UT-Austin: Minimum Security Standards for Data Stewardship

NIST Special Publication 800-57:

Recommendation for Key Management, Part 1 and Recommendation for Key Management, Part 2

Portions adapted from *University of Pittsburgh: Security Guidelines for Encryption*

(http://technology.pitt.edu/documentation/Security_Guidelines/Encryption_Guideline-vs-2.0.pdf), with permission from the University of Pittsburgh, Pittsburgh, Pennsylvania 15260-3332

Portions adapted from *Encryption at the University of California: Overview and Recommendations* (http://www.ucop.edu/irc/itsec/uc/EncryptionGuidelinesFinal.html), with permission from the University of California Office of the President, Oakland, California 94607-5200.

McMaster University - Campus Technology Liaison glossary: www.mcmaster.ca/ctl/glossary.htm

PURPOSE

Surveillance equipment can be used by school boards/authorities to comply with responsibilities under the Education Act and the duties of its employees as set out in the Education Act and Regulations. School boards/authorities can use video surveillance and the resulting records for inquiries and proceedings related to maintaining the health, welfare and safety of students, staff, and visitors while on school board/authority property and the protection of school property.

Definitions

Personal Information - Recorded information about an identifiable individual which includes, but is not limited to, information relating to an individual's race, colour, national or ethnic origin, sex, and age.

Reception Equipment - Refers to the equipment or device used to receive or record the personal information collected through a video surveillance system, including a camera or video monitor or any other video, audio, physical, or other mechanical, electronic, or digital device.

Record - Any information however recorded, whether in print form, on file, by electronic means or otherwise and including photographs, film, microfilm, videotape, machine-readable record, and any record that can be produced from a machine-readable record.

Video Surveillance System - A video, physical, or mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing, or monitoring of individuals in school buildings and on school premises (per IPC Video Surveillance Guidelines). Within the school board/authority, the surveillance system includes hand-held, portable digital devices used by principals and vice-principals to record school incidents for investigative purposes. Additional components of the surveillance system include portable video cameras that are used to record incidents
on designated school buses from time to time as required.

Storage Device - Refers to a video tape, computer disk or drive, CD-ROM, computer chip, or other device used to store the recorded data or visual, audio, or other images captured by a video surveillance system.

Considerations Prior to Using a Video Surveillance System

Before deciding if a school or facility warrants a video security surveillance system, the school board/authority should consider the following:

- A video security surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable. Video surveillance should only be used once it has been determined that conventional methods of maintaining a safe and secure environment have proven not to provide the level of safety that is required.
- Verifiable and specific incidents of vandalism or safety concerns must exist prior to the installation of video surveillance equipment.
- The school board/authority should ensure that the proposed design and operation of the video surveillance system minimizes privacy intrusion to that which is absolutely necessary to achieve its required and lawful goals.

Notification of the Installation of a Video Surveillance System

The public, students, and staff members should be notified of video surveillance through clearly written signs prominently displayed in the main entrances of all school board/authority facilities that operate a video surveillance system.

Clearly written signs should be prominently displayed at the perimeter of surveillance areas so that students, staff, and the public have reasonable and adequate warning that surveillance is or may be in operation before entering any area under surveillance.

Signage will satisfy the notification requirements of the Acts, which include informing individuals of the legal authority for the collection of personal information; the principal purpose(s) for which the personal information is intended to be used; and the title, business address, and telephone number of someone who can answer questions about the collection. At a minimum, there should be a sign in place that notifies individuals of the recording and informs them that they may contact the school office with any questions. The remainder of the notice requirements under the Acts can be satisfied through information pamphlets available in the school office.

The school board/authority should endeavour to be as open as possible about the video security surveillance program in operation and, upon request, will make available to the public information on the rationale for the video surveillance program, its objectives, and the policies and procedures that have been put in place.

Students need to be informed by the school principal at the beginning of each school year that the school board/authority may be recording student behaviour on school property and/or school buses and need to be informed about the purposes of such practices.

Where video surveillance is used on a school site, students, parents, and guardians shall be informed of related policies and procedures as incorporated into the student handbook or agenda.

Where video surveillance is used on a school site, all teaching and non-teaching staff shall be informed of related policies and procedures as incorporated into the staff handbook.

Teaching and non-teaching staff should be informed of the purpose of video surveillance and the constraints on viewing or distributing records.

Locations of Equipment

Reception equipment and/or surveillance equipment, such as video cameras, should only be installed in identified public areas where video surveillance is a necessary and viable means of ensuring the safety of students, staff, and school property or a necessary and viable means of detection or deterrence of criminal activity.

Equipment should be installed in such a way that only spaces that have been identified as requiring video surveillance are monitored.

Cameras located internally should not be directed to look through windows to areas outside of the building.

Cameras placed outside on a school site should be positioned only where it is necessary to protect external property and school assets or to provide for the personal safety of individuals on school grounds and premises.

Cameras should not be directed to look through the windows of adjacent buildings or onto adjacent property.

Video surveillance should not be used in locations where the students, staff, and public have a reasonable expectation of confidentiality and privacy, such as washrooms, change rooms, and private conference/meeting rooms. Cameras may be located in adjacent corridors to monitor traffic into these areas.

If cameras are adjustable by operators, this practice should be restricted, if possible, so that operators cannot adjust or manipulate the cameras to overlook spaces that are not intended to be covered by the video surveillance program.

Video monitors should not be located in an area that allows for public viewing.

Transportation Vehicles

A school board/authority may equip school buses and other school board/authority vehicles which are owned, leased, contracted and/or operated by the school board/authority with video recording devices for monitoring student behavior.

Video recording devices may be in operation on a temporary basis or rotated between vehicles without prior notice to students, as deemed necessary by the Manager of Transportation.

Video recording devices may be installed on vehicles used for the transportation of students when the administrators have received complaints of inappropriate behaviour or have reason to believe that behaviour problems exist or are about to occur.

Any agreements between the school board/authority and service providers shall state that the records dealt with or created while delivering a video surveillance program are under the school board's/authority's control and subject to the Acts.

Service providers and employees of service providers are required to review and comply with these procedures and the Acts in performing any duties and functions related to the operation of the surveillance system used on transportation vehicles.

The Manager of Transportation or designate is responsible for establishing procedures to ensure that its employees and transportation service providers use, collect, secure, retain, and dispose of recorded information in accordance with this policy and the Acts.

Secure Transmission

Information transmitted by the video surveillance equipment must be transmitted in a secure manner.

Use a wired video surveillance system, which inherently prevents interception, or a wireless surveillance system with appropriate measures, such as strong encryption, to preclude unauthorized access.

Wireless communication technology is not to be used unless strong, privacy-protective precautions have been used.

Maintenance

The school principal or site manager is usually responsible for ensuring that all surveillance equipment is maintained and serviced regularly.

Imaging equipment should be periodically inspected to ensure that video cameras and recording equipment are operating properly according to manufacturers' specifications.

Any issues or concerns regarding the performance of such equipment should be followed up with immediately.

Use, Disclosure, Retention, Security, and Disposal of Surveillance Records

Any information obtained through video surveillance systems may only be used for the purposes set out by MFIPPA and must relate to the protection of students, staff, and the public, including the discipline or consequences that arise from that, or it must assist in the detection and deterrence of criminal activity and vandalism. Information should not be retained or used for purposes other than those described above.

All recorded images are the property of the school board/authority and are used, disclosed, retained, secured, and disposed of in accordance with MFIPPA.

Circumstances that warrant a review shall be limited to instances where an incident has been reported or observed or to investigate a potential crime.

Video surveillance should not be used for monitoring staff performance.

The school principal or site manager should be responsible to manage, supervise, and audit the use and security of cameras, monitors, tapes, computers used to store images, computer diskettes, or all other video records related to the site.

The Manager of Transportation or designate shall be responsible to audit the use and security of surveillance cameras on school buses, including monitors and tapes.

Video records may never be sold, publicly viewed, or distributed in any other fashion, except as provided for by this policy and the appropriate legislation or as otherwise required by law or as evidence in a criminal or disciplinary proceeding.

Access to the storage devices should be limited to authorized personnel.

Images collected should only be viewed by the principal or vice-principal of the school, site manager, or the Superintendent of Education and/or in co-operation with members of the police.

The principal or site manager must authorize access to all video records other than those requested by the police. Without authorization by the principal or site manager, video records will only be released to or viewed by the police after school staff has been provided with a valid warrant.

When investigating specific incidents, the principal or vice-principal may enlist the aid of staff in the identification of individuals.

Disclosure of video records should be on a need-to-know basis, in order to comply with the school board's/authority's policy objectives, including the promotion of the safety and security of students, the protection of school board/authority property, and deterrence and prevention of criminal activities.

Video records may be released to third parties or applicants in conformance with the provisions contained in the *Freedom of Information and Protection of Privacy Act* (FIPPA) of Ontario and any rules or regulations thereunder or as otherwise required by law.

A log should be maintained by the principal, site manager, or designate of all episodes of access to or use of the recorded materials, to provide for a proper audit trail.

Recorded images shall be released to the police on request to aid in law enforcement in accordance with MFIPPA.

A storage device release form should be completed before any storage device is released to authorities or third parties. Any such release shall be made only in accordance with applicable legislation. The form will indicate the individual or organization who took the device, under what authority, when this occurred, and if it will be returned or destroyed by the individual or organization after use. This activity will be subject to audit and strictly enforced.

Video monitors for real-time monitoring shall be located in a protected area to prohibit unauthorized viewing by the public. Monitors can only be viewed by the principal, vice-principal, or designate. Real-time viewing of monitors may be delegated by the principal or Director of Education to a very limited number of individuals (e.g., a secretary or a special event security guard).

Video surveillance monitors shall not be viewed in real time in order to enforce school rules unrelated to the purposes of this policy. Real-time viewing of camera monitors is only permissible for limited duration when required for specific safety and protection issues.

Reception equipment should be located in a strictly controlled access area. Only controlling personnel or those properly authorized in writing by those personnel should have access to the controlled access area and the reception equipment.

Any agreements between the school board/authority and the service provider should state that the records dealt with or created while delivering a video surveillance program are under the school board's/authority's control and are subject to the Acts.

Vendors and/or service providers of the school board's/authority's video surveillance equipment shall not have access to recorded information.

Recorded images that have not been viewed or used for investigation should be retained for a standard period of time, typically one month. Recorded information that has not been used in this fashion is to be routinely erased every 30 days in a manner in which it cannot be reconstructed or retrieved.

Recorded information that has been viewed or used in the investigation of an incident shall be retained for a period of one year from the date viewed or one year from the date of resolution of the incident.

The principal or site manager must ensure that video records are disposed of in a secure manner.

Old storage devices must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved. Destruction methods for tapes and diskettes may include magnetic erasure, shredding, or incineration.

The Storage Device Disposal Record shall be completed when disposing of a storage device.

All recorded tapes and other storage devices that are not in use should be stored securely in a locked receptacle located in a controlled-access area as designated by the school principal or site manager. Each storage device that has been used shall be dated and labeled with a unique identifier, sequential number, or other verifiable symbol.

Access to Personal Information

Individuals who have been recorded by surveillance systems have the right to request access to their personal information under the Acts.

Parents, guardians, or employees requesting to view a segment of a video record involving their child(ren) or themselves may do so under the *Freedom of Information and Protection of Privacy Act* legislation.

Access may be granted to one's own personal information in whole or in part, unless an exemption applies under MFIPPA or FIPPA.

Access to an individual's personal information in whole or in part may be refused where disclosure would constitute an unjustified invasion of another individual's privacy. Access to an individual's personal information in these circumstances may depend upon whether any exempt information, such as other individuals in the video, can reasonably be severed from the record.

Should it become necessary to allow a parent or guardian to view a videotape where the confidentiality of others must be protected, the following options will be considered:

- Seek permission from the other party(s)
- Digitally enhance the tape to block the identity of the person(s)

This viewing must be done in the presence of an employee designated by the superintendent. The parent has the right to request an advocate to be present.

Principals should consult with their superintendent and/or the Freedom of Information/Records Management Coordinator regarding requests for access.

Training of Staff

Training programs addressing staff obligations under the Act shall be conducted.

The school principal or site manager is responsible for ensuring that all staff with access to surveillance equipment are trained, comply with, and understand their obligations under the Acts and related procedures.

Staff with responsibilities for the operation of the video surveillance equipment will receive training as to the permissible uses and the protections against inadvertent disclosure or retention.

Auditing and Evaluating the Use of Surveillance

The school board/authority will ensure that the use and security of video surveillance equipment is subject to regular audits. These audits will address the school board's/authority's compliance with the operational policies, guidelines, and procedures. An external body may be retained in order to perform the audit. The school board/authority will endeavour to immediately address any deficiencies or concerns identified by the audit.

Employees and service providers should be aware that their activities are subject to audit and that they may be called upon to justify their surveillance interest in any given individual.

The school board/authority will regularly review and evaluate its video surveillance program to ascertain whether it is still justified. This shall include an assessment of whether the deployment of cameras at a particular school remains justified. This evaluation shall occur at least once every three years and will include the review/update of associated policy, procedures, and guidelines.

Covert Surveillance

Covert surveillance occurs when surveillance devices are used without notification to the individuals.

Covert surveillance shall only be used in specific limited circumstances as an investigative tool related to criminal or illegal activity.

This type of surveillance will only be used when all other methods of dealing with the situation have been exhausted, and following the completion of a comprehensive assessment of the privacy impacts.

The benefits of capturing the information must outweigh the violation of privacy of the individuals observed. Covert surveillance will only be used with the approval of the superintendent of education and with the support of the police and will be time-limited.

Covert surveillance equipment shall be positioned in such a way as to minimize surveillance. For example, if equipment is being stolen or vandalized, individuals should only be recorded if they approach the equipment.

After a suspect has been identified, the surveillance equipment shall be removed.

The school board/authority should develop a protocol that establishes how the decision to use covert surveillance is made on a case-by-case basis. The protocol would also include privacy protection practices for the operation of the system.

Privacy Breach Response

Any inadvertent disclosure of personal information must be reported immediately to the Freedom of Information/ Records Office, Director of Education.

Sample Notifications

The following sample might be posted in main entrance of the school:

THE USE OF VIDEO SURVEILLANCE IS IN EFFECT

Surveillance systems are in operation to reduce/prevent vandalism, theft and violence and to ensure the safety of students, staff and others.

Information collected is collected by the *School Board* under the authority of the *Education Act* in accordance with the Municipal Freedom of Information and Protection of Privacy Act. For information, contact the school principal or the Freedom of Information/Records Management Coordinator of the *School Board, address, (XXX) XXX-XXXX - ext XXXX.*

Notice in Facilities

Entrances other than the main entrance, fence signage, and notification in facilities shall be:

THE USE OF VIDEO SURVEILLANCE IS IN EFFECT

Questions regarding this surveillance should be directed to the principal of the school.

Notice in School Handbook - Secondary

The *School Board* uses surveillance equipment used in secondary school facilities and school buses to:

a) enhance the safety of students and staff;

b) protect school property against theft or vandalism;

c) aid in the identification of intruders and of persons who endanger the health, well-being, or safety of school community members.

Information collected is collected by the *School Board* under the authority of the Education Act in accordance with the Municipal Freedom of Information and Protection of Privacy Act. For information, contact the school principal or the Freedom of Information/Records Management Coordinator of the *School Board, address, (XXX) XXX-XXXX - ext XXXX.*

Notice in School Handbook - Elementary

School board buses may from time to time use video surveillance as required.

FORM A
Log Sheet – Viewing of Recorded Images

	Date of Viewing (yyyy/mm/dd)	Date Recorded (yyyy/mm/dd)	Tape No./ ID #	Camera No./ Name	Surveillance Period	Type of Incident Reviewed	Incident Saved to Computer HD/CD-R /VCR	Police Notified of the Incident	Name of Person Viewing Recorded Images	Signature of Person Viewing Recorded Images
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Audit Conducted (Date/Time): _____

Auditor (Name – Printed): _____

Audit Organization (Name – Printed): _____

Signature of Lead Auditor: _____

FORM B
Log Sheet – Recorded Images Removed from School/Location via CD-R, Printed Copy, or VCR Cassette

	Date Removed (yyyy/mm/dd)	Date Recorded (yyyy/mm/dd)	Tape No./ ID #	Camera No./ Name	Surveillance Period	Type of Incident	Format of Image (CD-R, VCR Cassette, Print	Officer Name/ Badge/Occ #	Police Officer's Signature	Name and Signature of Person Releasing the Information
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										

Audit Conducted (Date/Time): _____

Auditor (Name – Printed): _____

Audit Organization (Name – Printed): _____

Signature of Lead Auditor: _____

FORM C
Log Sheet – Disposal of Recorded Information

	Date of Disposal (yyyy/mm/dd)	Time of Disposal	Date Recorded (yyyy/mm/dd)	Tape No./ ID #	Camera #/ Name	Surveillance Period	Type of Incident	Type of Device (CD-R, VCR tape)	Method of Disposal	Name of person disposing of recorded information	Signature of person disposing of recorded information
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

Not applicable for the routine overwrite/erasure of unviewed recorded material.

School Or Facility: _____

Audit Conducted (Date/Time): _____

Auditor (Name – Printed): _____

Audit Organization (Name – Printed): _____

Signature of Lead Auditor: _____

VIDEO SECURITY SURVEILLANCE SYSTEM STORAGE DEVICE RELEASE FORM

Date (yyyy/mm/dd)	**Time**	**Storage Device ID #**	**Form #**
Name of School/Facility	**Location of Storage Device** ☐ In-Use _____ ☐ Used _____	**Type of Device** ☐ Tape ☐ CD ☐ Disk ☐ Other (Specify) _____	
Name of Authorized Board Individual Releasing Storage Device (Print) **Position**		**Signature**	
Name of Individual Taking Custody of Storage Device (Print)		**Signature**	
Position	**ID or Badge Number**	**Organization and Telephone Number**	
Purpose or Reason For Release			
Disposition Following User: ☐ To Be Destroyed	☐ To Be Returned to School/Facility of Origin ☐ Other (Specify) _____		

An individual Storage Device Release Form is to be completed for each device to be released.
Copies to be made and distributed as required.

References

1. Information and Privacy Commissioner - *Guidelines for Using Video Surveillance Cameras in Schools* (2003)
2. Simcoe County District School Board - *Surveillance Systems, Administrative Procedures*
3. Windsor-Essex Catholic District School Board - *Video Security Surveillance Policy*
4. Kawartha Pine Ridge District School Board - *Video Surveillance, Administrative Regulations*
5. Avon Maitland District School Board - *Video Surveillance, Administrative Procedure No. 525*

PURPOSE

The purpose of this document is to provide recommendations on the proper use of videoconferencing for school boards with a focus on privacy and security issues. School boards/authorities should develop a more complete policy or guideline on the use of videoconferencing within their school board/authority in order to make effective use of the technology.

Definition

A **videoconference** is a set of *interactive telecommunication* technologies which allow two or more locations to interact via simultaneous two-way video and audio transmissions.

Benefits of Using Videoconferencing

School boards/authorities benefit through the proper utilization of a videoconferencing system. Videoconferencing can be used by administrators and other staff to conduct meetings, professional development, and interviews. Videoconference technology also allows for sessions to be recorded for future use, which may include instructional or promotional activities; however, it is important that the requirements of the *Municipal Freedom of Information and Protection of Privacy Act* be addressed prior to recording a videoconference.

Videoconferencing offers various possibilities for program delivery to students including virtual field trips, discussing lifestyle and culture with students in other countries, and sharing of educational resources. Videoconferencing reduces travel time, cost, and safety-related issues associated with travel.

Risks of Using Videoconferencing

Videoconference sessions open a window to the classroom or meeting room; therefore, staff must ensure that they know who is participating in the videoconference. Additionally, because videoconferencing technology allows for recording of conference sessions, it is important that controls are put in place to ensure that the conference is not recorded unless appropriate steps and measures have been put in place.

Personal Information

Personal information is defined in the *Municipal Freedom of Information and Protection of Privacy Act* and includes any information about an identifiable individual except for business title and contact. A simple image on a video system that is clear enough to identify a person or the activities in which they are engaged is classified as personal information and is protected under the Acts.

Appropriate steps need to be taken to ensure that personal information is protected whenever videoconferencing is used.

Confidential Information

Beyond the risk of exposing personal information there is also the risk of exposing confidential school board/authority information if the equipment is not used correctly or properly secured.

Inappropriate Content

It is possible for videoconferencing to be used for activities that are unsuitable for students. It is important that students are properly supervised and that connections are only made with trusted and approved sites to ensure activities are appropriate and to ensure student safety.

Inadvertent Release or Disclosure of Information

Sound and images that are broadcast could be captured as snapshots or videos from the system at the other location to which it is connected. If the broadcast is not encrypted, it could be intercepted. The video could then be posted to the Internet or otherwise used for purposes for which it was not intended.

General Guidelines

- Videoconferencing will not be used in any way to upload, post, reproduce, or distribute any information, software, or other material protected by copyright or any other intellectual property right without first obtaining the permission of such right holder.
- Videoconferencing systems will not be used for surveillance, either live or recorded.
- Staff using the videoconferencing system should be provided with training in advance so that they are familiar with the features and are aware of the security and privacy issues.
- Videoconferencing sessions shall not be recorded in any way or in any medium without the written permission of all individuals involved. Copyright and privacy legislation may be breached if images, video, or sound are recorded without permission or if recordings are used for purposes other than those agreed to, or in any other form or medium.
- Recorded information shall only be used for the purpose for which consent was provided.
- Video recordings are property of the school board/authority.
- Where videoconferencing is used to record a public meeting (e.g., a board meeting), meeting participants and the general public should be notified that the session is being recorded and informed of how it will be used. Notification shall include the intended use of the recorded images and the use of such records shall be limited to the purpose identified at time of recording.
  - Sample wording: "Please be advised that your image will be captured [optional: "and recorded"] during the proceeding videoconference. This information is collected under s. of the Education Act for the purposes of providing educational programming [optional: "it may be used in the classroom for the purposes of assisting in instruction"]. Questions about the collection may be addressed to [title] at [business address] or [business telephone number].

- Videoconferencing should be conducted on the school board/authority-approved videoconferencing system. Videoconferencing should not be conducted using personal equipment over the public Internet as this is difficult to control and increases the security and privacy risks associated with videoconferencing.
- Videoconferencing systems need to be secure to prevent unauthorized users or hackers from gaining access to the system and transforming the videoconferencing system into video surveillance units by viewing, recording, or publicly broadcasting presumably private videoconferences.
- The camera should never be left on when set to "Auto-Answer." If there is doubt as to the camera settings, the camera should be turned off when not in use.
- Ask the people at the other end of the videoconference who is in the room or listening to the videoconference. Sometimes the cameras do not have a wide enough view to show everyone in the room.
- Use the "Mute" feature when you are not speaking during a multi-point conference or when talking amongst yourselves before a conference starts.
- If possible, arrange for a phone to be nearby so that in the event of technical problems you can call and discuss the problem without leaving the room.
- Keep a videoconferencing session record or log to record when a session took place, who organized it, and who was involved.
- Know how to "stop" or "hang up" the call so that the videoconferencing session can be terminated if you are unhappy with the content.

Videoconferencing for Staff

- Staff will be notified prior to attending meetings or other events where videoconferencing is to be used. The notification should include information on who will be participating in or viewing the event.
- If the videoconference is to be recorded, staff must be made explicitly aware that the conference is being recorded and of the purposes for which the recording is to be used.

Video Conferencing Involving Students

- Schools must take responsibility for informing parents or guardians that videoconferencing with other schools or an external organization is being used by teachers with the students.
- It is recommended that schools collect written parental consent where the school where the videoconference is with external groups [**may require explicit consent depending upon when and why conferencing**].
- Where the videoconference is internal to the school board/authority, a notification letter to the parents may be sufficient unless the conference is being recorded [**notice should be sufficient even if recorded unless professional services**].
- Where videoconferences are arranged with external groups, it is important that the external group be approved by the school board/authority and school principal prior to the start of the conference.
- Prior to the start of the videoconference, external parties shall sign an agreement which sets out restrictions regarding access to the videoconference and the recording of the videoconference. Where conferences are recorded, the agreement shall clearly identify the purpose and use of the recording. Video recordings shall only

be used for the purpose identified in the consent form.

- All videoconferences should be approved in advance by the school principal. The school shall keep an annual log of sessions including date, time, and with whom the session is held.
- Schools must take responsibility for all students and any other individuals involved in video conferencing sessions.
- Students shall not be allowed to use videoconferencing equipment unsupervised by a teacher or learning assistant. The teacher should assume the normal role as class teacher and shall not assume that the presenter is able to see everything that is happening in the classroom. Any issues with behavior must be controlled by the class teacher, not the presenter.
- Students should not use headsets, as these may not allow adequate teacher assistance or supervision.
- Videoconference sessions with students shall not be recorded in any way or by any media, not consistent with the Act without the written permission of all individuals involved and the permission of a superintendent.

References

Cumbria and Lancashire Education Online - *Videoconferencing Acceptable Use Policy*

PURPOSE

This document outlines some legal considerations regarding video conferencing and includes sample contract wording that can be used when preparing video conferencing agreements between parties.

General Considerations

From time to time, school boards/authorities and individual schools may engage in video conferencing for a variety of purposes; these may include:

- Board staff video conferencing between board facilities
- Board staff video conferencing with external advisors or other service providers
- Teachers and students conferencing with their counterparts at other board schools
- Teachers and students conferencing with their counterparts at schools outside of the board
- Teachers and students conferencing with external service and/or content providers

The use of video conferencing may involve the collection of personal information about the participants and may therefore be subject to regulation under the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

MFIPPA regulates the collection, use, disclosure, security, and retention of personal information. Personal information is defined in part under the Act to mean information about an identifiable individual. It has been found to include information collected about individuals in the form of photographs and video images.

MFIPPA permits the collection of personal information such as video images where it is necessary for the proper administration of a lawfully authorized activity. Video conferencing that is necessary for conducting school business or is an important part of the delivery of an educational program will normally meet this criterion.

MFIPPA also requires that individuals whose images will be collected as part of a video conference be given proper notice of the collection under s.29 of the Act. This includes providing: (a) notice of legal authority, (b) a description of the purpose(s) of the collection, and (c) the title, business address, and business phone number of a board/authority representative who can answer questions about the collection (this will normally be the individual responsible for initiating the video conference).

A sample notice is set out below. The content of such notice will depend on the purpose of the collection and how it will be used/disclosed:

> Please be advised that your image will be captured [optional: "and recorded"] during the proceeding video conference. This information is collected under s. _____ of the Education Act for the purposes of providing educational programming [optional: "and it may be used in the classroom for the purposes of assisting in instruction"]. Questions about the collection may be addressed to [title] at [business address] or [business telephone number].

Notice may be provided at or before the time of the collection.

Restrictions on Use or Disclosure

MFIPPA requires that personal information should normally only be used for purposes identified in the collection notice, unless individuals have provided consent for the information to be used for other purposes, or unless one of the other exemptions under MFIPPA applies. Should you have questions about the appropriate use of a video conference recording, please contact the board's/authority's information and privacy coordinator.

Security

MFIPPA requires that personal information be secured in a reasonable manner to prevent its loss or unauthorized use or disclosure. Normally such recording should be stored in a locked container (desk, cabinet, etc.) by the person responsible for its maintenance.

From time to time, the school board/authority may retain external companies to provide video conferencing services or rely upon the external conferencing party to collect and record such data. Steps should be taken to apprise third parties of the board's/authority's obligations under MFIPPA and to secure agreement from such companies or external conferencing parties to handle any collected personal information in accordance with the requirements of the Act. A draft agreement is attached at the end of this policy as Appendix "A."

In addition, it is possible that external conferencing parties may wish to record conferences for their own purposes. In order to best protect the privacy of the participants (students, teachers, staff), the board/authority should obtain clear agreement with the conferencing party regarding the issue of recording (i.e., whether recording will be permitted and how any such recordings will be used). A second draft agreement is attached at the end of this policy as Appendix "B."

Retention

MFIPPA requires that personal information such as video conference recordings be retained for a minimum of one year from their use, unless one of the limited exemptions which permit shorter retention periods applies. If the personal information is not recorded during the video conference, this requirement is not applicable.

Access

Video conference recordings are subject to the access provisions of MFIPPA. Any formal access requests made for such recordings should be forwarded to the board's/authority's privacy coordinator for consultation and response.

Summary

While of tremendous benefit, video conferencing for students and staff can introduce a level of risk to privacy under the provisions of MFIPPA. Please refer to the "Guidelines for Videoconferencing" for additional information.

APPENDIX A
Agreement for Third Parties Providing Video Conferencing Services to the Board

The _____ board (the "board")

wishes to retain _____ for the purposes of providing video conferencing services

[or]

The _____ board (the "board")

wishes to rely upon _____ for the purposes of providing video conferencing services

The purpose(s) of the video conferencing is/are as follows (check applicable purposes):

☐ To facilitate instruction within the classroom.

☐ To facilitate instruction between the classroom and other groups (e.g., classes in other schools).

☐ To facilitate meetings between board staff.

☐ To facilitate external communications between board staff and external parties.

☐ To record the above noted conference(s).

☐ Other [describe]: _____

As you are aware, the board is subject to the Municipal Freedom of Information and Protection of Privacy Act.

In order to ensue the board's obligations under the Act are met, we ask that you confirm your agreement to comply with the following requirements, to which the board is subject, when handling personal information (as defined by the Act) pursuant to a retainer from one or more of the board's schools:

(i) _____ will collect only personal information necessary to administer the services retained by the school.

(ii) _____ will only use or disclose personal information for purposes consistent with the stated
purposes for its collection or as otherwise permitted by law and authorized by the board.

(iii) _____ will take all reasonable measures to prevent unauthorized access, loss or theft of personal information. _____ will notify the board immediately of any such event.

(iv) Upon request of the board, _____ will return or destroy any personal information in any form it maintains as necessary to provide the stated services.

(v) _____ will notify the board of any access request or request for correction made for personal information collected by _____ on behalf of the board.

Please confirm your agreement to comply with these requirements by returning a signed copy of this letter.

I, _____ on behalf of _____

acknowledge the legal requirements imposed on the board and agree on behalf of _____ that the company will comply with the requirements identified above when handling personal information on behalf of the board. I understand that failure to do so may result in a discontinuance by the board of the company's services.

APPENDIX B
General Agreement for External Conferencing Parties

The _____ board (the "board")

and _____ ("external party") wish to conduct a video conference (check applicable purpose(s)

☐ To facilitate instruction within the classroom.

☐ To facilitate external communications between board staff and external parties.

☐ Other [describe]: _____

In order to ensue the board's protects the privacy interests of the conference participants, the conferencing parties agree (check applicable opition):

☐ That neither party shall record the video conference.

☐ That only the board shall record the video conference.

☐ That only the external party shall record the video conference, subject to restrictions in this agreement set out below.

☐ That both parties shall record the video conference subject to restrictions set out below.

Restrictions on Recording:

Where either party has authorization from the other to record the video conference as set out above, use and disclosure of the record will be restricted as follows:

☐ Recordings will only used within the classroom for instructional purposes by each party.

☐ No copies of recordings will be permitted without express written consent of the other party.

☐ Images or other information from recordings will not be published or disseminated in any matter, including electronically or in print, without express written consent of the other party.

☐ Recording will be maintained in a secure manner so as to prevent theft or unauthorized access, use, or disclosure.

☐ Upon request by the other party, any recording will be destroyed.

☐ Each party will notify the other of any unauthorized access, theft, use, or disclosure.

As a condition of participating in the video conference, the parties agree to comply with the terms set out in this agreement,

Dated this _____ day of _____, 20____

_____

For the board

_____

For the external party

PURPOSE

The purpose of this guideline is to help school boards/authorities determine what information should be retained in accordance with their School Board/Authority Records and Information Management (RIM) Program.

What Is a Record?

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

The MFIPPA is an act to promote access to information held by government and to protect the privacy of personal information which provides the public with a right of access to records collected by government, subject to limited and narrow exemptions. It defines a record as follows:

A record is recorded information however recorded whether in printed form, on file, by electronic means or otherwise and includes correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof. It further states that any information that is capable of being produced by a machine and subject to the regulations any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution.

It is important to note that not all records will be released in response to a Freedom of Information Request. Contact your Freedom of Information Coordinator for more information.

International Standard Organization (ISO) Standard 15849 - Information and Documentation - Records Management

This standard defines a record as recorded information created, received, and maintained as evidence by an organization or person in pursuance of legal obligations or in the transaction of business. It requires that records:

- correctly reflect what was communicated or decided or what action was taken;
- support the needs of the organization; and
- support accountability.

Why Are Records Important?

Records are important for their content and as evidence of communication, decisions, actions, and history. As public institutions, school boards/authorities are accountable to the public and to government. Records support openness and transparency by documenting and providing evidence of work activities and by making them available to the public. Records support quality program and services, inform decision making, and help meet organizational goals.

What Activities and Transactions Should Be Documented?

Records include any information that documents the mission and planning objectives of the organization which include planning, decisions, actions, and results, as follows:

- results of significant daily activities that support the mission and objectives of our organizations;
- advice and recommendations made to management and the decisions and actions taken as a result, along with supporting documentation;
- problems encountered in organizational operations and the steps taken to resolve the problems;
- interactions with the public, customers, clients, stakeholders, consultants, vendors, partners, and other government jurisdictions;
- verbal communications such as meetings, telephone calls, and face-to-face discussions where significant actions or decisions have occurred;
- legal agreements of any kind, including contracts, along with supporting documentation;
- policy, organizational planning, performance measurement, and budget activities, and supporting documentation;
- work done for the government by consultants and other external resources; and
- actions and decisions where payments are made or received, funds committed, services delivered, or obligations incurred.

What Are Official Records?

Not all records and information need to be retained. Records and information that should be retained as part of a records management are records that:

- are required to support daily operations; or
- document and provide evidence of business transactions; or
- are required by legislation; or
- protect the rights of citizens and the government; or
- provide evidence of compliance with accountability or other organizational requirements; or
- will have some future organizational, financial, legal, research, or archival value to the government and public; or
- are personal information that has been used by the organization which is required to be retained pursuant to the legislation; or
- evidence of compliance with a duty/responsibility to report a child in need of protection.

Official records should be stored securely so that they will be readily available to those who need them and are authorized to access them. This applies in both our paper-based and our electronic work environments.

What Are Non-Records or Transitory Records?

Not all records created or received should be treated as official records. Some have no further value to the organization beyond an immediate or minor transaction. Others might be required only for a very short time, perhaps until they are made obsolete by an updated version of the record or by a subsequent transaction or decision.

Non-records or transitory records are not required to control, support, or document the delivery of programs, to carry out operations, to make decisions, or to account for activities of the department. Non-records should be managed and routinely disposed of in an appropriate manner once the administrative, legal, or fiscal use has expired. These non-records may include:

- **Advertising materials:** solicited or unsolicited information you receive from businesses or individuals advertising their products or services.
- **Blank information media:** blank information media, e.g., letterhead, blank CDs, etc.
- **Draft documents and working materials:** correspondence, reports, and other documents, which usually have not yet been finalized. These include research or working materials such as calculations and notes that are often collected and used in the preparation of documents. Once the final version of a document is complete and filed, most drafts and working materials should be disposed of.
- **Duplicate copies** where nothing has been added changed or deleted, where the copy is used for information or reference only, and where the original is filed in the records management system.
- **External publications:** books, magazines, periodicals, pamphlets, brochures, journals, newspapers, and software documentation, whether printed or electronic, that you have obtained from sources outside your organization. Publications that are about schools or school boards/authorities may have historical value and should be retained as part of the records management program.
- **Routine notices:** notices that contain information useful for only a brief period of time, after which it has no further value or is of little interest. Note that the originating department is responsible for retaining the notice if it supports departmental activities, responsibilities, or communication.
- **Information of short-term value/unsolicited information:** information received as part of a distribution list, or email messages received from listservs and other Internet sources, solely for convenience of reference.

When Should Non-Records or Transitory Records Not Be Disposed of?

Any information that may relate to a Freedom of Information Request or to pending litigation or legal discovery should not be destroyed until finalized. In addition records containing personal information must be maintained for a minimum of one year from use unless a shorter period is authorized under MFIPPA.

What about Email?

Over time, email has evolved from an electronic message delivery system to a repository of records and non-records. It is important to remember that any information contained in an email or an email repository that meets the definition of a record as defined in this document must be managed as part of the organization-wide records management program. School boards/authorities need to develop policies and procedures to ensure that these are managed as part of the records management program.

Characteristics of a Record

The International Standard Organization (ISO) Standard 15849 - Information and Documentation - Records Management defines the characteristics of a record. In addition to demonstrating accountability, a record should support organizational needs.

Records Should Have:

- **Content:** A record should reflect what was communicated or decided or what action was taken, and should provide enough information so that it is understood.
- **Context:** It should reflect how it was used or why it was created (purpose), the date, the time, and the participants.
- **Meaning:** It should be linked to other documents or information to which it relates.

Authenticity

A record is one that can be proven:

- to be what it purports to be;
- to have been created or sent by the person purported to have created or sent it; and
- to have been created or sent at the time purported.

Reliability

Records must be trusted to be a full and accurate representation of the transactions, activities, or facts and can be relied upon in subsequent activities. To ensure reliability, records should be created at the time of the transaction or incident or soon afterwards and by individuals with direct knowledge of the facts.

Integrity

A record must be complete and unaltered and must be protected from unauthorized changes, and verifiable unaltered.

Usability

To be useable, records must be retrievable, presented, and interpreted. The links between other records should be maintained.

Summary

Records are a strategic organizational asset that must be managed. To manage them appropriately, staff must recognize that information has a lifecycle and that not all records and information must be retained.

References

1. *Official and Transitory Records: A Guide for Government of Alberta Employees*
2. *ISO Standard - 15849 - Information and Documentation - Records Management*

PURPOSE

The purpose of this guideline is to assist school board/authority employees in developing privacy notification statements for websites, along with forms (paper and electronic), emails, and facsimiles.

Privacy notification statements explain how personal information (i.e., information capable of identifying an individual) will be treated as individuals interact with a school board/authority or school. In addition, privacy notification statements assure both internal and external publics that the personal and confidential information they provide to a school board/authority and/or school will be handled appropriately. A privacy notification statement must be posted on all websites, paper and electronic forms, facsimiles, and emails which collect personal information in identifiable form-that is, information that is personal in nature and which may be used to identify an individual.

Examples of personal information: Name, date of birth, age, sex, gender, racial ethnicity, social insurance number, patient/physician ID, employee number, photo, voiceprint, fingerprint, home address/phone/email, educational background, financial transactions, medical history, criminal or employment history, or any other identifying number, symbol, or other identifying particular assigned to the individual.

School boards/authorities should document their position on the use of privacy notification statements within their board in order to make employees aware of their responsibilities relating to the collection, use, disclosure, and retention of personal and confidential information. To that end, this guideline is being put in place to ensure that the information contained in privacy notification statements is accurate and appropriate for the school board/authority and/ or school.

Overview

Privacy is a major concern of students, parents, school board/authority employees, volunteers and service providers. Concerns include a lack of transparency regarding the use and disclosure of personal information and about the security of their personal information.

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and the *Personal Health Information Protection Act* (PHIPA) govern the conditions under which school boards/authorities and/or schools may collect, use, and disclose personal information and how individuals must be informed when a school board/authority and/or school is collecting this information.

Schools and/or school boards/authorities have a wide variety of reasons for collection and use of personal information. For this reason, it is impossible to develop a single privacy notification statement for all circumstances personal information might be collected, used, and disclosed. This document is meant to provide guidance to school boards/authorities and school staff about different types of privacy notification statements that might be included, given a particular circumstance.

The purpose of collection will determine what kind of privacy notification statement you require. For example, a very simple form or website that just provides information may only require a general privacy notification statement. However, forms and websites that collect personal information from users need to ensure that the requirements of the MFIPPA and/or PHIPA are met. This guideline provides sample privacy notification statements from which school boards/authorities and/or schools can build a privacy notification statement that is appropriate for their circumstances. This document includes sample privacy notification statements to show what a complete privacy notification statement might look like.

Placement of a privacy notification statement is also a very important consideration. Guidelines on the placement of the privacy notification statement on a form, facsimile, and website are included.

Definition

Privacy notification statements outline the responsibilities a school board/authority and/or school has regarding collection, use, disclosure, and retention of personal and confidential information in order to inform internal and external individuals. MFIPPA at s.28(2) states: "No personal shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity." MFIPPA at s.29(2) states: "If personal information is collected on behalf of an institution…shall inform the individual to whom the information relates of,:

a) the legal authority for the collection;

b) the principal purpose or purposes for which the information is intended to be used; and

c) the title, business address and business telephone number of an officer or employee of the institution who can answer the individual's questions about the collection."

In addition, this guideline recommends that, if possible, school boards/authorities and/or schools also include the following information:

- where/how the information will be stored;
- the retention period;
- who will use the information; and
- who will get copies of the information.

Guidelines

- The Privacy Notification Statement must be inserted at the point at which an individual is asked to provide the information.
- Developing a website privacy notification statement is not easy. The end result should help users to underst and what information is being collected about them and how it is to be used. Moreover, the privacy notification statement should reflect the school board's/authority's and/or school's actual organizational practices and how the website is operated technically.
- Privacy notification statements must occur whenever personal information about an identifiable individual is captured or recorded. All data collected must be needed for each individual from whom it is collected.

- A school board/authority and/or school may use personal information only to the extent necessary to enable the school board/authority and/or school to carry out the activity for which it was collected in a reasonable manner.
- Privacy notification statements should be printed on every collection form itself, whether paper or electronic, and on a separate or covering document that is a guide to the completion of the form, if applicable.
- Privacy notification statements should not be shaded and the type size should allow the notification to be clearly readable with average vision, preferably of the same type size as the rest of the body of the form.
- The design of forms should place the privacy notification statement either at the top of the form (before any personal information is collected) or at the bottom of the form just above the signature line.
- Personal information must be retained for a minimum of one year following the use of the information. If it is retained longer to satisfy the retention period then the longer of the two need to be stated on the form.
- When developing privacy notification statements, include expertise from IT, the school board's/authority's Freedom of Information/Protection of Privacy Coordinator, the school board's/authority's Records Manager, communications staff, and staff from the program area. If possible, also get legal counsel to participate in the process. Bringing together this expertise will ensure that:
- practices comply with the MFIPPA and/or PHIPA;
- program needs are met and IT processes are understood.
- Appoint one person (perhaps from Communications) to take responsibility for drafting. This way, the group can concentrate on the content, and "writing by committee" can be avoided.
- Consider submitting the final privacy notification statement to the legal counsel for the school board and, if appropriate, to the Communications department before finalizing and publishing it to your site. Consider having the privacy notification statement reviewed by the Office of the Information and Privacy Commissioner.

Developing a Website Privacy Notification Statement

- Before developing a privacy notification statement for the school board/authority and/or school website, consider how the website is used (e.g., broadcasting static information, providing customized entry points, conducting functions that collect personal information); think about the target audience and how knowledgeable they are about how websites operate; and the technical operation of your site (e.g., does it use cookies, what data is captured automatically).
- Websites change constantly with respect to new content and function. Consider reviewing the privacy notification statement regularly to ensure that it is still appropriate.
- A link to the privacy notification statement must be provided from every page of the website.
- School board/authority and/or school stakeholders are knowledgeable about privacy issues; therefore, consider giving prominence to the privacy notification statement on the home page. This is an increasingly frequent practice among private and public sector organizations to show their commitment to protecting the privacy of users.
- If users can conduct transactions on the site (for example, filling out a form or application), provide a link to the general privacy notification statement for the website. As well, a specific privacy notification statement should be created regarding the use and authority for the information to be collected on the form, just as it would on paper-based transactions with stakeholders.

- A good website privacy notification statement contains multiple parts. Each part addresses specific concerns of users or specific aspects of personal information that may be collected depending on how the website is built and operated and how the users use the site.
- Use the chart below to determine what parts need to be included in your privacy notification statement. You will notice that many of the parts will be appropriate to most sites. These parts are identified with a check mark.
- By using this checklist, you can ensure that the school board's/authority's privacy notification statement reflects both how its site is used and its operational practices.

Key Parts of a Web Site Privacy Notification Statement

Which of the following situations apply to your Web site?		Build your own Privacy Notification Statement using these models.
You are primarily posting information and need a broad general Privacy Notification Statement.	☑	General Privacy Notification Statements
You collect usage statistics automatically.	☑	Information Collected and Stored Automatically
Your site is monitored for security protection.	☑	Security
Your site provides links to other sites.	☑	Privacy and Links to Other Sites
Your site enables visitors to submit information through emails and web forms.	☐	Information Collected in Emails and Web Forms
Your site includes transactions (e.g., online forms, applications) where personal information enters a system of records in your organization.	☐	Transactions Where Information Enters a System of Records
Users may ask for information about who to contact about your privacy policy.	☑	Getting More Information

General Website Privacy Statements

Websites can provide a first impression of the school board/authority and/or school. A clearly presented general policy on privacy can reassure users that the information you collect about them will be handled appropriately. General privacy notification statements are appropriate for sites that only post information-where users are browsing, searching, and downloading information from the site. General privacy notification statements should be written in plain language and tell users what, if any, information is collected when they visit the site. If the site does not use cookies or other tools for collecting user information, it is wise to state this in the general privacy notification statement. Here are two examples of 'general' privacy notification statements.

Example 1:

We are committed to providing our visitors with a Web site that respects their privacy. This page summarizes the privacy policy and practices of the (NAME OF SCHOOL BOARD/AUTHORITY/SCHOOL) Web site.

We do not automatically gather any personal information from you, such as your name, phone number, email or address. This information is only obtained if you supply it voluntarily, usually through contacting us via email or registering in a secure portion of the site.

Any personal information you do provide is managed according to the Municipal Freedom of Information and Protection of Privacy Act. This means that, at the point of collection, you will be informed that your personal information is being collected, the purpose for which it is being collected and that you have a right of access to the information.

This Web site does not use "cookies" or any other means of collecting information about you or your computer without your knowledge. (A "cookie" is a file placed on your hard drive by a Web site that allows the Web site to monitor your use of the site, usually without your knowledge.)

Example 2:

Thank you for visiting the (NAME OF SCHOOL BOARD/AUTHORITY/SCHOOL) Web site and reviewing our privacy policy. Our privacy policy is clear: We will not collect personal information about you when you visit our Web site unless you choose to provide that information to us.

We do not regularly use "cookies" to track how our visitors use the site. Whenever we enable "cookies" to facilitate your transactions, we will first inform you.

Here is how we handle information about your visit to our Web site: (INSERT APPROPRIATE NOTES).

Information Collected and Stored Automatically

Often, websites routinely collect information about visitors to assess traffic and usage of a site. School boards/authorities might have the technical capability to collect information and later take additional steps to identify people (e.g., looking up static Internet Protocol (IP) addresses that may be linked to specific individuals).

Privacy notification statements should state clearly what information you are collecting automatically. More importantly, your statement should reflect whether you intend to make this information identifiable, or to use it only for statistical purposes.

If the school board/authority and/or school site is using cookies, the privacy notification statement should state how it is using cookies (e.g., persistent cookies or session cookies.)

Example 1:

Here is an example of a simple privacy notification statement reflecting the fact that one's IP address is not used to link activity to a particular individual.

The (NAME OF SCHOOL BOARD/AUTHORITY) uses software that receives and records the Internet Protocol (IP) address of the computer that has contacted our Web site.

We make no attempt to link these addresses with the identity of individuals visiting our site.

Example 2:

You may want to be more specific about the type of information that is collected automatically during a visit to the site, as in the following example.

If you do nothing during your visit but browse through the website, read pages, or download information, the (NAME OF SCHOOL BOARD/AUTHORITY) will automatically gather and store certain information about your visit. This information does not identify you personally. We automatically collect and store only the following information about your visit:

- the Internet domain (for example, "xschoolboard.ca" if you use a private Internet access account) and IP address (an IP address is a number that is automatically assigned to your computer whenever you are surfing the Web) from which you access our website;
- the type of browser and operating system used to access our site;
- the date and time you access our site;
- the pages you visit; and
- if you linked to the (NAME OF SCHOOL BOARD/AUTHORITY) website from another website, the address of that website.

The (NAME OF SCHOOL BOARD/AUTHORITY) uses this information to help us make our site more useful to visitors-to learn about the number of visitors to our site and the types of technology our visitors use. We do not record information about identifiable individuals and their visits.

Example 3:

Not all IP addresses can be tracked to an individual. The following statement reflects this fact.

When you visit the (NAME OF SCHOOL BOARD/AUTHORITY) website, the web server automatically collects a limited amount of information essential for the operation and security of our website and the other sites that reside on the server. Some of this information (e.g., browser type) does not identify who you are. Other information, such as your Internet domain name or IP address, may identify you depending, in large part, on the naming standards followed by your Internet service provider.

Example 4:

The following statement acknowledges that personal information may be collected but not used to identify an individual. It is based on the vocabulary of the World Wide Web Consortium's Privacy Preferences Project (P3P). A P3P standard is not yet finalized. Because of its technical nature, this type of statement may be more suited to a knowledgeable group of users.

(NAME OF SCHOOL BOARD/AUTHORITY/SCHOOL) logs http requests to our server. These logs capture computer information and navigation and click stream data, such as the originating IP (e.g., 204.41.227.10) address of an agent requesting a URL and the email address of the site visitor if they have included it in their browser. This data is used in non-identifiable form for website and system administration purposes.

Logged information is not disclosed outside of (NAME OF SCHOOL BOARD/SCHOOL) personnel or those under contract to conduct maintenance to web server components. The logs are permanently archived as raw research material. The logs may not be accessed, opted out of, or changed by server users.

A user may have questions about who has access to information collected, as outlined above. It might be appropriate to include information about when the MFIPPA and PHIPA might permit disclosure of information that can be made identifiable. Moreover, even if the information is intended to be used internally, there might be cases where school boards/authorities are required by law to surrender the files. Users should be told of this possibility.

On these issues, it is wise to consult the school board's/authority's legal counsel to ensure that the privacy notification statement accurately reflects actual practice or likely practice in the near future.

Example 5:

The following example clearly states that no one will have access to personal information except in cases where the school board is required to disclose the information.

The (NAME OF SCHOOL BOARD/AUTHORITY) records your visit and logs the following information for statistical purposes-your server's address; the name of the top-level domain from which you access the Internet (for example, .gov, .com, .ca, .org, etc); the type of browser you use; the date and time you access the site; the pages you have accessed and the documents you have downloaded, and the previous Internet address from which you linked directly to the site.

We will not identify users or their browsing activities, except as required by a law of Ontario or Canada or if we are compelled to produce this information for a legal proceeding.

Cookies are a common method of collecting information about users. If your site uses cookies, you should be explicit about:

- how you are using the cookies;
- how long the cookie will reside on their machine; and
- how the user can reject the cookie or disable this function.

Example 6:

The following example is one that has been reviewed by the Alberta Office of the Information and Privacy Commissioner and is currently used on the Travel Alberta website. It states that cookies are being used. It describes what a cookie is and how it is used on the site. It also describes how the user can disable the cookie. Finally, it is explicit about how long the cookie will reside on the user's machine.

This website uses "cookies." Cookies are small amounts of information that are distributed to web browsers to assist you when you return to this site or a specific area on the site. The cookie used here retains session information, or more specifically, the options selected to determine your itinerary. If you have concerns about this, you can change the settings on your web browser to not accept this information or to display warning messages when this is about to occur. Cookies are not retained by the site but reside on your machine and are marked for removal by your browser after a period of 28 days.

Example 7:

The following example is more explicit about how the cookies are used on the site. In this case, the cookie expires 30 minutes after the last time the cookie was modified.

We only enable "cookies" for our searchable Frequently Asked Questions (FAQ) database, and then only for the feature that allows you to register to be notified when a question is modified. A cookie is a small piece of text information that is sent to your browser-along with a Web page-when you access a website. Your browser will only return this cookie information to the domain where the cookie originated. No other site can request it.

In the case of our searchable FAQ database, the cookie helps us remember you if you request to be notified of a change of a question. If you choose to disable cookies, you may still request that you be notified when a question is changed, but you will be required to enter your email address for every question you wish to be notified about. The cookie will expire 30 minutes after the last time the cookie was modified. This expiration time does not delete the cookie from your PC, but it does make it invalid and we can no longer use that cookie. No other website can use this cookie under any circumstances. If you wish to delete this (or any cookie), that is a function of your web browser and you should consult the software's Help files.

Example 8:

It may also be helpful to tell people what the impact of disabling the cookie will be, as in the following example.

(NAME OF SCHOOL BOARD/AUTHORITY WEBSITE) does not use persistent cookies (persistent tokens that pass information back and forth from the client machine to the server). We do use session cookies (tokens that remain active only until you close your browser) in order to make the site easier for you to use. We DO NOT keep a database of information obtained from these cookies.

We use cookies in the following ways:

- To save you time in filling out forms. When you close your browser, the cookie is deleted from your computer.
- To maintain a relationship between the image and the correct link, the program that displays the banners on the bottom of some of our pages uses a session cookie. When you close your browser, the cookie is deleted from your computer.

You can choose not to accept these cookies and still use the site, but it may take you longer to fill out the same information repeatedly and clicking on the banners will not take you to the correct link. Refer to the help information in your browser software for instructions on how to disable cookies.

Security

School board/authority websites are usually monitored to maintain system security. Your privacy notification statement should contain a statement related to this activity.

Example 1:

The following example notifies the reader of the maintenance of usage logs and how they may be accessed. It also identifies how long the logs are maintained.

For site security purposes and to ensure that this service remains available to all users, this (NAME OF SCHOOL BOARD/AUTHORITY) computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits.

Privacy and Links to Other Web Sites

One of the advantages of the Web is the ability to link to other information. Almost all school board/authority websites have links to other organization, agency and/or government sites as well as non-government sites. In these cases, the privacy notification statement should contain a notice to the user that if they go to another site from yours, the privacy policy of that site may be different.

Example 1:

The following example states that the school board/authority is not responsible for the privacy policy of other sites that it may be linked to. It also encourages users to look at the privacy policy of sites they visit.

This website contains links to other sites. We are not responsible for the content and the privacy practices of other websites and encourage you to examine each site's privacy policy and disclaimers and make your own decisions regarding the accuracy, reliability, and correctness of material and information found.

Example 2:

Sometimes, your site may warn the user that they are leaving your site. If this is the case, the following example tells the user that the school board/authority cannot be responsible for the practices of linked sites, but that they will be warned before leaving your site.

Our website has links to many other sites. Before leaving the (NAME OF SCHOOL BOARD/AUTHORITY) website, a page will appear informing you that you are leaving our server. Once you link to another site, you are subject to the privacy policy of the new site. You should review the privacy policy and disclaimers of the new site you are going to.

Information Collected in E-mails and Web Forms

Most school board/authority websites allow the user to email an employee of the department (e.g. "feedback" to the webmaster). Many sites also have forms that users can fill out to receive further information, become part of a mailing list or listserv, or join a discussion group.

Almost all of these instances involve the collection of personal information. The privacy notification statement should clearly state how this information is to be used, if and how it will be retained, and to whom (and in what form) it may be disclosed.

It is also a good practice to warn the person that, while the information submitted will be protected once is reaches your site, the Internet is not totally secure and that you cannot ensure that the information will be protected during transmission to your site.

Example 1:

In the following example, the use of the personal information submitted is described. It also describes who has access to this information.

If you join an (NAME OF SCHOOL BOARD/AUTHORITY) online discussion group, we may ask you to volunteer personal information such as your name and email address for the purposes of effective administration of the discussion group. In some cases, our groups are limited to member-only discussions and as such can not be accessed by the general public. We will notify you as to whether you are joining a closed (limited) or open (public) discussion.

Any personal information you supply will not be disclosed to anyone except (NAME OF SCHOOL BOARD/AUTHORITY) personnel who need the information (e.g., to respond to your request).

Example 2:

The following example explains that emails are treated the same way as letters sent to your organization.

If you choose to provide us with personal information-as in an email or by filling out a form with your personal information and submitting it to us through our website-we use that information to respond to your message and to help us get you the information you have requested.

We treat emails the same way we treat letters sent to (NAME OF SCHOOL BOARD/AUTHORITY). We only share the information you give us with another school board department if your inquiry relates to that department.

Moreover, we do not create individual profiles with the information you provide or to give it to any private organizations. (NAME OF SCHOOL BOARD/AUTHORITY) does not collect information for commercial marketing.

Example 3:

The following example warns users that the information they provide may not be secure before it reaches your site.

Messages sent via the Internet can be intercepted. If you are concerned about sending your personal information to us via the Internet, you can use another method such as fax or regular mail. For more help, call (NAME OF SCHOOL BOARD/AUTHORITY) at (TELEPHONE NUMBER).

Transactions where Information Enters a System of Records

As more and more school boards/authorities use the Internet to carry out transactions with stakeholders, personal information protected by the MFIPPA and PHIPA will be collected. In these instances, it is good practice to conduct a Privacy Impact Assessment (PIA).

In cases where traditional paper collections of information are supplemented or replaced by electronic forms offered through a website, the rules of the MFIPPA and PHIPA continue to apply.

For situations where a notice is required in the paper-based world, the general principle is that the equivalent notice is required in the online world. You should have a link to the appropriate privacy notification statement at the point where the information is collected.

In these cases, as with current practices in service delivery that do not involve the Internet, the MFIPPA and PHIPA place restrictions on what information may be collected.

Web visitors also like to know how long their personal information is kept.

Example 1:

In the following example, the privacy notification statement contains a generic reference to the MFIPPA and PHIPA. The example also states (in general terms) how the information will be used and how long it will be kept.

The information provided on this application is for the purpose of determining eligibility for the (Autistic Student CASA Program) under s. _____ of the Education Act and will be retained for _____. If you have any questions regarding the collection of this information, please contact (title of an individual) within Special Education Services at the address or phone number provided.

Example 2:

We are collecting this personal information to determine and verify your eligibility for Special Education programs. We do so pursuant to s.170(1) of the Education Act. Your personal information is protected by the privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act and the Personal Health Information Protection Act and will be retained for _____. If you have any questions about the collection of this information, you may contact (title of an individual) within Special Education Services at (Area Code) (Telephone Number).

Example 3:

Any personal information that we ask you to provide via our website is collected in compliance with the Municipal Freedom of Information and Protection of Privacy Act and/or the Personal Health Information Protection Act. We collect only what is necessary for the operation of the website and the provision of requested materials to you. The information is used only for the purpose it was collected or for a consistent purpose. Further, we keep the information only for the length of time necessary to fulfill the purpose for which it was collected or one year, whichever is shorter.

Getting More Information

There may be users that have concerns or questions about the school board's/authority's privacy policy. Therefore, it is a good idea to include information about whom to contact if the user has questions.

Here are two examples of simple statements that can be used at the end of your privacy notification statement to help users who may have questions.

Example 1:

For more information about any of the policies described above or about our school board website in general, please contact us:

- By email: (EMAIL ADDRESS)
- By telephone: (TELEPHONE NUMBER)
- By fax: (FAX NUMBER)

Example 2:

If at any time you have questions about our privacy policy, please notify the Freedom of Information /Protection of Privacy Coordinator for the school board by email at (EMAIL ADDRESS).

If you do not wish to send your request using email, you can send it in writing to the following postal address: (INSERT ADDRESS).

Sample Privacy Notification Statements for Websites

Here are two sample privacy statements that were developed to meet specific needs of particular sites. They are included here to give you an idea of how different parts of the privacy notification statement can be put together to form a cohesive, easy-to-read statement.

Example 1:

The (NAME OF SCHOOL BOARD/AUTHORITY) has developed this site as a resource for individuals wanting information about the (NAME OF SCHOOL BOARD/AUTHORITY). We are committed to providing our visitors with a website that respects their privacy. This page summarizes the privacy policy and practices on the (NAME OF SCHOOL BOARD/AUTHORITY) websites.

We do not automatically gather any personal information from you, such as your name, phone number, or email address. This information is only obtained if you supply it voluntarily, usually through contacting us via email, or registering in a secure portion of the site.

Any personal information you do provide is protected under the Municipal Freedom of Information and Protection of Privacy Act and/or the Personal Health Information Protection Act. This means that, at the point of collection, you will be informed that your personal information is being collected, the purpose for which it is being collected, and that you have a right of access to the information.

We use software that receives and records the Internet Protocol (IP) address of the computer that has contacted our website. We make no attempt to link these addresses with the identity of individuals visiting our site.

We do not regularly use "cookies" to track how our visitors use the site. Whenever we enable "cookies" to facilitate your transactions, we will first inform you.

Visitor information is not disclosed to anyone except the (NAME OF SCHOOL BOARD/AUTHORITY) personnel who need the information, e.g., to respond to a request.

This website contains links to other sites. We are not responsible for the content and the privacy practices of other websites and encourage you to examine each site's privacy policy and make your own decisions regarding the accuracy, reliability and correctness of material and information found.

For questions or comments regarding this policy, or for additional information about the administration of the (NAME OF SCHOOL BOARD/AUTHORITY), please visit our website at www.xxxxxxxx or contact us:

- By email: [Email Address]
- By telephone: [(Area Code) Phone Number]
- By fax: [(Area Code) Fax Number]

Example 2:

Privacy commitment

The (NAME OF SCHOOL BOARD/AUTHORITY) respects the privacy of our stakeholders. We pledge to never release your personal information (i.e., name, address, telephone number, email address) to anyone who is not employed or contracted by us to provide a service to you. We will only use this information to serve you better.

The (NAME OF SCHOOL BOARD/AUTHORITY) may from time to time, with your permission, send you information we feel will be of use to you. If you prefer not to receive this type of information in the future, just let us know by contacting us (see below) and we will take you off our mailing list.

Information collected via the Internet

When you visit the (NAME OF SCHOOL BOARD/AUTHORITY) website, the web server automatically collects a limited amount of information essential for the operation and security of our website and the other sites that reside on the server. Some of this information (e.g., browser type) does not identify who you are. Other information, such as your Internet domain name or IP address, may identify you depending, in large part, on the naming standards followed by your Internet service provider. You may wish to ask them about their policies and practices in this regard.

Messages sent via the Internet can be intercepted. If you are concerned about sending your personal information to us via the Internet, please call the (NAME OF SCHOOL BOARD/AUTHORITY) at (Area Code) (Telephone Number, Ext.).

Cookies

This website uses "cookies." Cookies are small amounts of information that are distributed to web browsers to assist you when you return to this site or a specific area on the site. The cookie used here retains session information, or more specifically, the options selected to determine your itinerary. If you have concerns about this, you can change the settings on your web browser to not accept this information or to display warning messages when this is about to occur. Cookies are not retained by the site but reside on your machine and are marked for removal by your browser after a period of 28 days.

What other personal information we collect and how we use it

Any personal information that we ask you to provide via our website is collected in compliance with the Municipal Freedom of Information and Protection of Privacy Act and/or the Personal Health Information Protection Act. We collect only what is necessary for the operation of the website and the provision of requested information to you. The information is used only for the purpose for which it was collected or for a consistent purpose. Further, we keep the information only for the length of time necessary to fulfill the purpose for which it was collected. (State any information here) information is collected, stored, and used only in non-identifying form.

Links to other websites

This site contains links to other educational related websites. We are not responsible for the privacy practices of any sites you may visit after you enter the (NAME OF SCHOOL BOARD/AUTHORITY) site.

Questions?

For more information about any of the policies described above or about our website in general, please contact us:

- By email: [EMAIL ADDRESS]
- By telephone: [(AREA CODE) TELEPHONE NUMBER]
- By fax: [(AREA CODE) FAX NUMBER]

Example 3:

The (NAME OF SCHOOL BOARD/AUTHORITY) is committed to respecting your privacy and protecting your personal information. This privacy sStatement explains the current information management practices on our websites.

The handling of all personal information by the (NAME OF SCHOOL BOARD/AUTHORITY) is governed by the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), the Personal Health Information Protection Act (PHIPA), and the Education Act.

What kind of information is collected when you visit our websites?

When you browse or download information from the (NAME OF SCHOOL BOARD/AUTHORITY) website, our servers automatically collect limited amounts of standard information for traffic monitoring and statistical purposes. The information is analyzed for operational trends and performance and for ways to improve the site. Examples of this type of information include:

- Internet Protocol (IP) address of the computers being used;
- dates and times our site is accessed;
- types and versions of the browsers used to access our sites and the operating systems of the computers being used;
- pages visited;
- names of the files requested.

In addition, we may use the IP address to address any potential security threats.

What happens when you give personal information online to the (NAME OF SCHOOL BOARD/AUTHORITY)?

If you chose to voluntarily provide us via email with personal information, such as your name, address, phone number, or email address, to allow us to follow up on in an inquiry, any such information that you provide to us will be used to respond to your specific question.

If you would prefer to write, please send your letter to:

- The FOI/Records Manager
  NAME OF SCHOOL BOARD/AUTHORITY
  Address, Phone, Email Address, Fax

Does the (NAME OF SCHOOL BOARD/AUTHOIRY) use "cookies"?

A "cookie" is a small text file that a website can store on your computer's hard drive to collect information about your activities on the site or to make it easier to use certain site functions. The cookie transmits this information back to the website's computer when you visit the site. If you do not want cookies stored on your computer, you can set your browser to warn you when a website attempts to place a "cookie" on your computer. For instructions on how to do this refer to website browser.

The (NAME OF SCHOOL BOARD/AUTHORITY) does/does not use cookies on its public website. (If so, why and when.)

Does the (NAME OF SCHOOL BOARD/AUTHORITY) link to other websites?

Some of our websites link to other websites created and maintained by other public and/or private sector organizations. These links are provided solely for your information and convenience. When you link to an outside website, you are leaving the (NAME OF SCHOOL BOARD/AUTHORITY)'s site and are subject to the privacy and security policies of that site's owners. You are encouraged to read their privacy statements to understand how they handle personal information.

The (NAME OF SCHOOL BOARD/AUTHORITY) does not assume and is not responsible for any liability whatsoever for the linking of any of these linked websites, the operation or content (including the right to display such information) of any of the linked websites, nor for any of the information, interpretation, comments or opinions expressed in any of the linked websites. Any comments or inquiries regarding the linked websites are to be directed to the particular organization for which the particular website is being operated. Students are encouraged to consult with their parents before they link to an outside site.

Accuracy of Content

This information is provided as a public service. Although we endeavor to ensure that the information is as current and accurate as possible, errors do occasionally occur. Therefore, we cannot guarantee the accuracy of the information. Readers should, where possible, verify the information before acting on it.

Whom can I contact for further information about my privacy on this site?

Questions or comments regarding this statement may be directed to our (NAME OF SCHOOL BOARD/AUTHORITY) Freedom of Information/Protection of Privacy Coordinator or by phone at (Area Code) Phone Number, Ext., Email Address, Fax Number.

Example 4:

The (NAME OF SCHOOL BOARD/AUTHORITY) respects the privacy of its web visitors. Personal information on the Internet is protected in the same way it is protected in all other ways that are communicated and interacted with. Staff should adhere to strict policies that protect the confidentiality of any personal identifiable information such as names, email addresses and telephone numbers. The use of cookies is strictly prohibited except to provide data on a performance measure of meeting informational or service needs relative to the Internet site. The only

personal identifying information collected from use of the school board/authority website is from submitting comments, suggestions, or questions through a feedback form or an email. The school board will not sell, rent, or release personal information to third parties.

Example 5:

The (NAME OF SCHOOL BOARD/AUTHORITY) is committed to providing our staff, students, and visitors with websites that respect their privacy. This page summarizes the privacy policy and practices for all (NAME OF SCHOOL BOARD/AUTHORITY) websites. (NAME OF SCHOOL BOARD/AUTHORITY) websites do not automatically gather any personal information from you, such as your name, phone number, or email address. This information is only obtained if you provide it voluntarily through contacting us via email or via an online form. Any personal information you do provide is managed according to the Municipal Freedom of Information and Protection of Privacy Act and/or the Personal Health Information Protection Act. This means that, at the point of collection, you will be informed that your personal information is being collected, the purpose for which it is being collected, and that you have a right of access to the collected information. Some (NAME OF SCHOOL BOARD/AUTHORITY) websites may collect more information than is described here and will have additional privacy policies. Where applicable, please be sure to read these privacy policies.

Information Collected Automatically via the Internet

The (NAME OF SCHOOL BOARD/AUTHORITY) logs http requests to our server. These logs capture computer information, navigation and click stream data.

Some of the information collected does not identify who you are. Other information, such as your domain name or IP address, may identify you depending on the naming standards followed by your Internet service provider.

<u>You may wish to ask them about their policies and practices.</u>

While we make no attempt to link the information captured to the identity of individuals, the information captured does identify the following:

1. the Internet domain and IP address from which you access our website;
2. the type of browser and operating system used to access our site;
3. screen resolution of your monitor;
4. the date and time you access our site;
5. the pages you visit; and
6. if you linked to the (NAME OF SCHOOL BOARD/AUTHORTIY) website from another website, the address of that website.

This information is used to help us make our site more useful to our audiences by learning about the number of visitors to our site and by monitoring traffic patterns and the types of technology our visitors use. We do not track or record information about specific individuals and their visits. Visitor information is not disclosed to anyone except (NAME OF SCHOOL BOARD/AUTHORITY) personnel who need the information for legitimate purposes such as responding to a request.

Cookies

A cookie is a small piece of text information that is sent to your browser when you access a website. Your browser returns this cookie information to the domain where the cookie originated. While we do not regularly use cookies to track how our visitors use the site, when cookies are used, they may be used to help you fill in forms or track your use of the sites. The length of time that the cookie resides on your machine depends upon the specific setup of the particular sites you visit. If you are concerned about the use of cookies, you can refer to the help information in your browser software for information on how to disable cookies. If you wish to delete cookies from your machine, consult your browser's help files for instructions on how to do so.

Cookies Used on Some Sites

A number of (NAME OF SCHOOL BOARD/AUTHORITY) websites (such as the one you are viewing now) use dynamically driven content. These pages use two specific cookies to define the parameters of the site you are visiting. These tokens are identified by your browser as CFIDE and CFTOKEN. These cookies do not gather or submit any information on users visiting the site.

Security

For site security purposes, the (NAME OF SCHOOL BOARD/AUTHORITY) employs software programs to monitor network traffic in order to identify unauthorized attempts to upload or change information or to otherwise cause damage. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits.

Privacy and Links to Other Sites

(NAME OF SCHOOL BOARD/AUTHORITY) websites may contain links to other sites. We are not responsible for the content and the privacy practices of other websites and encourage you to examine each site's privacy policy and disclaimers and make your own decisions regarding the accuracy, reliability, and correctness of material and information found.

Information Collected in Emails and Web Forms

If you should choose to provide us with personal information-as in an email or by filling out a form and submitting it to us through our website-we will use that information to respond to your message and to help us get the information you have requested. The (NAME OF SCHOOL BOARD/AUTHORITY) does not collect personal information for commercial marketing or distribution to any private organizations.

Messages sent via the Internet can be intercepted. If you are concerned about sending your personal information to us via the Internet, you can use another method such as fax or regular mail.

Transactions Where Information Enters a System of Records

Where personal information is provided that enters a system of records, it is collected in compliance with the Municipal Freedom of Information and Protection of Privacy Act. The (NAME OF SCHOOL BOARD/AUTHORITY) collects, creates, and maintains information for the purposes of admission, registration, and other activities directly related to its education programs. Information collected is only kept for the length of time necessary to fulfill the purpose for which it was collected.

Getting More Information

For questions or comments regarding this policy, or for additional information about the administration of the Municipal Freedom of Information and Protection of Privacy Act and Personal Health Information Protection Act, contact the Freedom of Information and Privacy Coordinator for the (NAME OF SCHOOL BOARD/AUTHORITY).

Links

(NAME OF SCHOOL BOARD/AUTHORITY) Freedom of Information/Protection of Privacy Coordinator
Privacy Statement Guidelines for (NAME OF SCHOOL BOARD/AUTHORITY)

Policy Statement

In the normal course of operation, the (NAME OF SCHOOL BOARD/AUTHORITY) generates and collects a significant amount of confidential information about current and former staff, students, and parents, as well as about (NAME OF SCHOOL BOARD/AUTHORITY) operations. The purpose of this policy is to promote safeguarding of, and controlling access to, confidential information; to prevent inadvertent disclosure of confidential information; and to protect the privacy of individuals and the integrity and reputation of the (NAME OF SCHOOL BOARD/AUTHORITY). The primary purpose of this policy is to make sure that the school board/authority does not inadvertently disclose confidential information.

Access to and disclosure of confidential information held by the (NAME OF SCHOOL BOARD/AUTHORITY) must be allowable, appropriate, necessary, and for a clearly defined purpose. No information should be provided to any person who does not have the right to access personal information without the signed consent of that individual.

Website Terms of Use

The following statement may be considered for use when developing a website privacy notification statement.

Example 1:

This website is maintained by (NAME OF SCHOOL BOARD/AUTHORITY) as a public service to students, parents, staff and site visitors from the community and beyond. The (NAME OF SCHOOL BOARD/AUTHORITY) cannot guarantee that all information is current or accurate. Website users should verify all information before acting on it. The (NAME OF SCHOOL BOARD/AUTHORITY) reserves the right to change or modify its terms, conditions, and notices under which use of the website is offered. Continued use of this website constitutes an agreement to all such terms, conditions, and notices.

Communications made through this website's email and messaging system should in no way be deemed to constitute legal notice to the (NAME OF SCHOOL BOARD/AUTHORITY) or any of its agencies, officers, employees, agents, or representatives, with respect to any existing or potential claim or cause of action against the (NAME OF SCHOOL BOARD/AUTHORITY) or any of its agencies, officers, employees, agents, or representatives.

Sample Privacy Notification Statements - Forms

The Statement for the Authorization for Collection of Personal Information on both paper and electronic forms should include:

- Purpose for the collection - why do you need this personal information?
- What legislation entitles us to collect this information?
- Where will the information be stored?
- How long will the information be kept?
- Who will use the information?
- How or why they will use the information.
- Who can be contacted to answer questions regarding this collection?
- Who will get copies of this personal information?

Here are two sample privacy notification statements that can be used on forms (both electronic and paper). They were developed to meet specific needs of particular sites. They are included here to give you an idea of how different parts of the privacy statement can be put together to form a cohesive, easy-to-read statement.

Example 1:

MFIPPA Notification Statement (minimum type size - 8 pt.):

The personal information requested on this form is collected under the authority of the Municipal Freedom of Information and Protection of Privacy Act and will be protected under that Act. It will be used for the purpose of (state specific uses for which the information is collected, authorized by [IDENTIFY STATUTE AND STATUTE SECTIONS - i.e., Education Act s._____]). Direct any questions about this collection to: (contact position, full address, and business telephone number).

Example 2:

Information Collection Authorization:

This information is collected pursuant to the board's responsibilities as set out in the section(s) _____ of the Education Act and the Municipal Freedom of Information and Protection of Privacy Act. The information will be used for educational purposes and stored in the Ontario Student Record (OSR) for 5 years after the student graduates or completes their education, unless otherwise removed in accordance with the Education Act. The information will be used by the principal, classroom teacher and central office Special Education Department staff for the purposes of _____. Questions about this collection should be directed to the principal of the school.

Copies: 1. OSR 2. Parent (upon request)

Sample Privacy Notification Statement - Email and Facsimile

This email contains information intended only for the individual or entity named in the message. If the reader of this message is not the intended recipient or the agent responsible to deliver it to the intended recipient, you are hereby notified that any review, dissemination, distribution, or copying of this communication is prohibited. If this communication was received in error, please notify us by reply email and delete the original message.

Sample Privacy Notification Statement - Facsimile

This fax contains information intended only for the individual or entity named in the message. If the reader of this message is not the intended recipient or the agent responsible to deliver it to the intended recipient, you are hereby notified that any review, dissemination, distribution, or copying of this communication is prohibited. If this communication was received in error, please notify us and destroy the original fax.

Conclusion

Privacy notification statements make employees aware of their responsibilities regarding the collection, use, disclosure, and retention of personal and confidential information. In addition, privacy notification statements assure both internal and external stakeholders that the personal and confidential information they provide to the school board/authority and/or school will be handled appropriately.

Developing privacy notification statements is not easy. Time and effort should be put into the development of privacy notification statements to ensure that they reflect the school board's/authority's actual operational practices.

Sources

Many of the examples used in this guide were adopted from websites that have developed their own privacy statements. Privacy statements from the following organizations were useful in developing the examples used in this guide:

- The University of Alberta
- Australian Sports Commission
- Industry Canada
- Office of the Information and Privacy Commissioner (Ontario)
- Office of the Information and Privacy Commissioner (Alberta)
- U.S. Department of Defense
- U.S. Department of Justice
- Peterborough Victoria Northumberland and Clarington Catholic District School Board
- Toronto District School Board - Privacy Complaint No. MC06-63
- Simcoe County District School Board
- World Wide Web Consortium's Privacy Preferences Project (P3P)

PURPOSE

This protocol is designed to help Ontario school boards/authorities contain and respond to incidents involving unauthorized disclosure of personal information.

The ability to address privacy breaches will be greatly improved by implementing a standardized, consistent management approach such as suggested in these guidelines. Everyone has a role and responsibility to assist in the containment of a privacy breach.

Benefits of a Privacy Breach Protocol

- Quick and coordinated response;
- Clarified roles and responsibilities;
- Effective investigation process;
- Effective containment process;
- Easier remediation.

Notice to Readers

Ontario school boards/authorities should adapt these guidelines to suit their particular operating norms. Legal advice or other expert assistance can, and should, be sought as required.

Definition of a Privacy Breach

A privacy breach occurs when personal information is compromised, that is, when it is collected, used, disclosed, retained, or destroyed in a manner inconsistent with privacy legislation. Ontario school boards/authorities are governed by the following privacy statutes: *Municipal Freedom of information and Protection of Privacy Act* (MFIPPA), *Personal Health Information Protection Act* (PHIPA), and *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Personal information can be compromised in many ways. Some breaches have relatively simple causes and are contained, while others are more systemic or complex. Privacy breaches are often the result of human error, such as an individual's personal information being sent by mistake to another individual (e.g., fax number, email address, etc.). In today's environment in which technology increasingly facilitates information exchange, sometimes a privacy breach can be more wide-scale, such as when an inappropriately executed computer programming change causes the personal information of many individuals to be compromised.

The following are some examples of privacy breaches:

	Student Records	Employee Records	Business Records
Inappropriate disclosure/use of personal information	Two teachers discussing (and identifying) a student in the local grocery store. Student's report card mailed to the wrong home address. Digital images of individuals taken and displayed without consent. Hard-copy psychological assessments kept in openly accessible file cabinets that are not secured or controlled. Confidential student health records inadvertently blown out of a car trunk and scattered over a busy street.	Employee files containing social insurance numbers left in unlocked boxes near the open shipping/receiving area. Budget reports (containing employee numbers and names) found in their entirety in recycle bins and garbage bins. Theft from car of a briefcase containing a list of home addresses of teaching staff.	A list of names, including credit card numbers, left on the photocopier. Personal information disclosed to trustees who did not need it to effectively decide on a matter.
Technology/ computer error	Lost memory key containing student data. Theft from teacher's car of a laptop containing Special Education student records on the hard drive.	Sending very sensitive personal information to an unattended, open-area printer. Password written on a sticky note stuck to a monitor. Resumes faxed or emailed to a wrong destination or person.	Stolen laptop containing names and addresses of permit holders. Tender information scanned and not cleared from multi-functional office machine. Disposal of equipment with memory capabilities (e.g., memory keys, disks, laptops, photocopiers, fax machines, or cell phones) without secure destruction of the personal information it contains.

Appendices

APPENDIX A – Responding to a Suspected Privacy Breach

Ontario school boards/authorities can use this appendix in the form of a poster to promote and raise the awareness of responsibilities in the event of a privacy breach.

APPENDIX B – FOI Coordinator Privacy Breach Checklist

This appendix is a recommended management tool for Ontario school boards'/authorities' Freedom of Information (FOI) Coordinators or designates to use in the event of a privacy breach.

Roles and Responsibilities in Responding to Privacy Breaches

The following personnel may need to be involved when an Ontario school board/authority responds to a privacy breach. Some of the following roles and responsibilities may be undertaken concurrently.

Individuals	Roles	Responsibilities
Employees	All Ontario school board employees need to be alert to the potential for personal information to be compromised, and therefore potentially play a role in identifying, notifying, and containing* a breach. Employees dealing with student, employee and/or business records need to be particularly aware of how to identify and address a privacy breach.	All Ontario school board employees have the responsibility to: • notify their supervisor immediately, or, in his/her absence, their school boards/authority's FOI Coordinator upon becoming aware of a breach or suspected breach; • contain*, if possible, the suspected breach by suspending the process or activity that caused the breach.
Senior Administration, Managers, and Principals	Senior administration, managers, and principals are responsible for alerting the FOI Coordinator of a breach or suspected breach and will work with the coordinator to implement the five steps of the response protocol.	Senior administration, managers, and principals have the responsibility to : • obtain all available information about the nature of the breach or suspected breach, and determine what happened; • alert the FOI Coordinator and provide as much information about the breach as is currently available; • work with FOI Coordinator to undertake all appropriate actions to contain the breach; • ensure details of the breach and corrective actions are documented.
FOI Coordinator	The FOI Coordinator plays a central role in the response to a breach by ensuring that all five steps of the response protocol are implemented (see pages 34-36 for more details).	The FOI Coordinator will follow the following five steps (see page 34-36 for more details): Step 1 - Respond Step 2 - Contain Step 3 - Investigate Step 4 - Notify Step 5 - Implement Change

Individuals	Roles	Responsibilities
Accountable Decision Maker	The responsibility for protecting personal information affected by a privacy breach is assigned to an identified position who is the accountable decision maker. This individual is the key decision maker in responding to privacy breaches and therefore needs to be familiar with the Ontario school boards/ authorities' roles, responsibilities and the response plan. In most Ontario school boards/authorities, the Director of Education is the accountable decision maker.	The accountable decision maker has the responsibility to : • brief senior management and trustees as necessary and appropriate; • review internal investigation reports and approve required remedial action; • monitor implementation of remedial action; • ensure that those whose personal information has been compromised are informed as required.
Third Party Service Providers	Increasingly, Ontario school boards/ authorities use contracted third party service providers to carry out or manage programs or services on their behalf. Typical third party service providers are commercial school photographers, bus companies, external data warehouse services, outsourced administrative services (such as cheque production, records storage and shredding), Children's Aid Societies (CAS), Public Health Units (PHU), external researchers, and external consultants. In such circumstances, Ontario school boards/authorities retain responsibility for protecting personal information in accordance with privacy legislation. Therefore, third party service providers need to know their roles and responsibilities if a privacy breach occurs when they have custody of personal information. All third party service providers must take reasonable steps to monitor and enforce their compliance with the privacy and security requirements defined in the contracts or service agreements, and are required to inform their respective Ontario school boards/authorities of all actual and suspected privacy breaches.	The third party service providers have the responsibility to: • inform the Ontario school board/ authority contact as soon as a privacy breach or suspected breach is discovered; • take all necessary actions to contain the privacy breach as directed by the Ontario school board/authority; • document how the breach was discovered, what corrective actions were taken and report back; • undertake a full assessment of the privacy breach in accordance with the third party service providers' contractual obligations; • take all necessary remedial action to decrease the risk of future breaches; • fulfill contractual obligations to comply with privacy legislation.

Everyone has a role and responsibility to notify and contain a privacy breach depending on the situation.

Response Protocol: Five Steps Implemented Concurrently by the FOI Coordinator.

Initiate these steps as soon as a privacy breach or suspected breach has been reported.

Step 1 - Respond

- Assess the situation to determine if a breach has indeed occurred and what needs to be done;
- When a privacy breach is identified by an internal or external source, contact the appropriate area to respond to the breach;
- Provide advice on appropriate steps to take to respond to the breach;
- Report the privacy breach to key persons within the Ontario school board/authority (including the Director of Education or designate) and, if necessary, to law enforcement;
- Evaluate effectiveness of response to the breach and implement improvement as necessary.

Step 2 - Contain

- Identify the scope of the breach and contain it (e.g., retrieve the hard copies of any personal information that has been disclosed, determine if the breach would allow unauthorized access to any other personal information [e.g., electronic information system], change passwords and identification numbers and/or temporarily shut down the system if necessary to contain the breach);
- Document the breach and containment activities;
- Develop briefing materials;
- Brief the accountable decision maker, senior management, and key persons on the privacy breach and how it is being managed.

Step 3 - Investigate

Once the privacy breach is contained:

- Conduct an investigation with the involvement of other parties as necessary:
  - Identify and analyze the events that led to the privacy breach;
  - Evaluate what was done to contain it; and
  - Recommend remedial action so future breaches do not occur.
- Document the results of internal investigation and use the privacy breach checklist for record keeping, including:
  - background and scope of the investigation;
  - legislative implications;
  - how the assessment was conducted;
  - source and cause of the breach;
  - inventory of the systems and programs affected by the breach;
  - determination of the effectiveness of existing security and privacy policies, procedures, and practices;
  - evaluation of the effectiveness of the Ontario school board's/authority's response to the breach;
  - findings including a chronology of events and recommendations of remedial actions;
  - the reported impact of the privacy breach on those individuals whose privacy was compromised.

Step 4 - Notify

- Notify, as required, the individuals whose personal information was disclosed;
- Refer to page 36, "How do you Determine if Notification is Required?"

The purpose of providing notice of a privacy breach to the individuals whose personal information was involved in the incident is to provide them with information about:

- what happened;
- the nature of potential or actual risks or harm;
- what mitigating actions the board is taking;
- appropriate action for individuals to take to protect themselves against harm.

If personal information that could lead to identity theft has been disclosed, affected individuals should be provided with information on steps they can take to protect themselves. If the office of the Information and Privacy Commissioner (IPC) is investigating the privacy breach, indicate that to the affected individuals. Give an explanation of the individual's right to complain to the IPC about the Ontario school board's/authority's handling of their personal information, along with contact information for the IPC.

- Notify appropriate managers and employees within your Ontario school boards/authorities of the breach;
- Report the privacy breach to the office of the Information and Privacy Commissioner (IPC) as appropriate.

Contact information:
Information and Privacy Commissioner/Ontario
1-800-387-0073
info@ipc.on.ca
www.ipc.on.ca

Step 5 - Implement Change

When determining what changes and remedial actions need to be implemented, consider whether it is necessary to:

- review the relevant information management systems to enhance compliance with privacy legislation;
- amend or reinforce the existing policies, procedures, and practices for managing and safeguarding personal information;
- develop and implement new security or privacy measures, if required;
- review employee training on legislative requirements, security and privacy policies, procedures, and practices to reduce potential or future breaches, and strengthen as required;
- test and evaluate remedial actions to determine if they have been implemented correctly and if policies, procedures, and practices need to be modified;
- recommend remedial action to the accountable decision maker.

How Do You Determine if Notification is Required?

The following factors should be considered when determining whether notification is required:

Risk Of Identity Theft

Is there a risk of identity theft or other fraud in your Ontario school board/authority? How reasonable is the risk? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with social insurance numbers, credit card numbers, driver's license numbers, personal health numbers, debit card numbers with password information, or any other information that can be used for fraud by third parties (e.g., financial).

Risk of Physical Harm

Does the loss or theft of information place any individual at risk of physical harm, stalking, or harassment?

Risk of Hurt, Humiliation, or Damage to Reputation

Could the loss or theft of information lead to hurt, humiliation, or damage to an individual's reputation? This type of harm can occur with the loss or theft of information such as mental health records, medical records, or disciplinary records.

Risk of Loss of Business or Employment Opportunities

Could the loss or theft of information result in damage to an individual's reputation, affecting his/her business or employment opportunities?

Sources

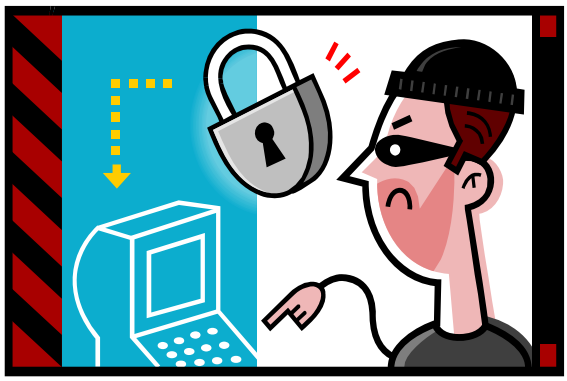
AICA/CICA Privacy Taskforce, *Incident Response Plan 2003*
(American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants)

Government of Ontario, Ontario Shared Services, *Privacy Review 2005*

Information and Privacy Commissioner/Ontario, *Breach Notification Assessment Tool, December 2006*

Information and Privacy Commissioner/Ontario, *What to do if a Privacy Breach Occurs: Guidelines for Government Organizations*, May 2003

The Office of the Chief Information and Privacy Officer, Taking the Right Steps - *A Guide to Managing Privacy and Privacy Breaches*, revised April 18, 2007



RESPONDING TO A SUSPECTED PRIVACY BREACH

PRIVACY is...

...the **right to control** access to your personal information, and the **right to decide** what and how much information you give to others, who it is shared with, and for what purposes.

A PRIVACY BREACH occurs when...

...personal information that is collected, used, disclosed, retained or destroyed in a manner **that does not meet privacy requirements** set out in federal and provincial privacy legislation.

Examples *of privacy breaches may include, but are not limited to: memory key/jump drive left in a public area containing student data; laptop lost or stolen containing student records on the hard drive; documents containing student or employee personal information left unattended on a photocopier; reports containing employee personal information found unshredded in recycle bins or garbage bins; confidential documents left in public view on an employee's desk or other publicly accessible area.*

If you suspect a PRIVACY BREACH has occurred, YOU are encouraged to...

...notify your Supervisor immediately, or, in his/her absence, your School Board's Freedom of Information (FOI) Coordinator at *(insert phone number of FOI Coordinator here);*

...contain, if possible, the suspected breach by delaying or stopping the process or activity involving the exposure or mishandling of student or employee personal information.

Following your report of the suspected breach, the FOI Coordinator may contact you to confirm details about the suspected breach.

No further action is required on your part unless further directed by your Supervisor and/or the Board's FOI Coordinator.

BREACH REPORT # _____

Take immediate action when you have been advised of a suspected privacy breach. Many of the steps outlined below have to be carried out simultaneously or in quick succession. Steps 1 and 2 are completed based on the information received either directly from an employee, or orally through his/her immediate supervisor (e.g., phone call), or in written form (e.g., email).

STEP 1 – Respond, and STEP 2 – Contain

1. Person Reporting Suspected Breach:

First name: _____ Last name: _____

Job title: _____

Location (school/department): _____

Name of immediate supervisor: _____

Phone number: _____

2. When Incident Occurred: Date: _____ Time: _____
(mm/dd/yyyy) (indicate A.M. or P.M.)

3. Incident Details:

Number of individuals whose information was accessed without consent or authorization: _____

Type of personal information that was accessed without consent or authorization, e.g., health/medical information, student marks, biographical information (such as home address, phone numbers, names and contact information of family members), behaviour concerns, etc. _____

_____

_____

Whom the personal information belongs to and **how many individuals were affected** (e.g., student, employee, third party [someone who is neither a student nor employee of the board, such as a parent/ guardian or volunteer]):

_____

_____

_____

Who had unauthorized access to the personal information, and **how** that access was made: _____

_____

_____

Efforts made, if any, to contain the privacy breach (e.g., suspending the process/activity that caused the breach)

_____

_____

Date: _____ Time: _____
(mm/dd/yyyy) (indicate A.M. or P.M.)

STEP 3 – Investigate

Following a report of a suspected privacy breach, ensure that the activity/process has been contained if possible. Conduct an investigation of the information supplied in Steps 1 and 2 of this report in conjunction with current privacy legislation (MFIPPA, PHIPA, PIPEDA) and with local privacy policies and procedures to determine if the incident is, in fact, a breach. Note: You may wish to consult legal counsel to assist you in your investigation.

If a breach HAS NOT occurred:

Contact the person who reported the suspected breach **and** his/her immediate supervisor to advise him/her of your determination. No further action is required by the employee or supervisor.

STEP 4 – Notify

If a breach HAS occurred:

Notify the following individuals as appropriate:

- ☐ Individuals whose privacy was breached
- ☐ Senior administration/managers/principals
- ☐ IPC*
- ☐ Accountable decision maker (Director of Education)
- ☐ Legal counsel
- ☐ Other

* **Note**: The type and extent of the breach will influence your decision to notify the Information and Privacy Commissioner's Office, Toronto (1-800-387-0073) 2 Bloor Street East, Suite 1400, Toronto, Ontario, M4W 1A8.

STEP 5 – Implement Change

Steps taken to correct the problem:

- ☐ Develop, change, or enhance policies and procedures
- ☐ Ensure strengthening of security and privacy controls
- ☐ Advise IPC of investigation findings and corrective action

Provide additional notices (as deemed appropriate):

- ☐ Relevant third parties
- ☐ Consider public announcement (e.g., statement and/or apology)
- ☐ Other Ontario school boards/authorities (where shared responsibilities exist)

Prevent future breaches:

- ☐ Arrange employee training on privacy and security
- ☐ Recommend appropriate and necessary security safeguards
- ☐ Consider having an outside party review processes and make recommendations (e.g., auditing company)
- ☐ Evaluate the effectiveness of remedial actions

The FOI Coordinator may wish to review school board/authority policies, procedures, practices, and training materials to ascertain whether any revisions are required to ensure a clearer understanding of what constitutes a privacy breach.

Sign-off

The Director of Education or designate (e.g., FOI Coordinator) is required to sign below to formally acknowledge that the breach was handled in accordance with privacy legislation and with the school board's/authority's policies and procedures:

_____ _____

Print Name/Title Signature

Sign-Off Date: _____
(mm/dd/yyyy)

PURPOSE

The *Education Statute Law Amendment Act* (Student Performance Bill 78), *2006, received Royal Assent on June 1, 2006. Introduced in March 2006, the act contains several limited but substantive amendments to the Education Act and the Ontario College of Teachers Act*, 1996, *to support improved student performance and cooperation between education service providers based on respect and openness to the public for the purpose of improved student performance.*

MISA (Managing Information for Student Achievement) is a provincial initiative designed to build local and provincial capacity to collect, manage, and access information to support evidence-informed decision making to improve student learning. In accordance with this initiative, school boards/authorities are developing systems for managing and accessing a wide range of data, enhancing the technology available for reporting and analysis, and providing increased access to data and information related to student achievement.

The Privacy and Information Management (PIM) taskforce was established in September 2006 as an OASBO (Ontario Association of School Business Officials) and MISA joint project committed to helping school boards comply with provincial and federal access and privacy legislation. The PIM taskforce also supports efforts to meet the expectations of parents, students, and teachers with respect to information security and protection of personal information, thereby strengthening public trust and confidence.

What is a Privacy Impact Assessment (PIA)?

A PIA is an assessment framework used to identify the actual or potential risks that a proposed or existing information system, technology, or program may have on an individual's privacy. Examples of such systems and programs include data warehousing, centralized electronic student information systems, and information sharing with other school boards/authorities, education providers, or sectors.

Completing a PIA will help school boards/authorities determine if there are privacy-related concerns and risks that can be mitigated. It can also assist in identifying:

- options for managing, minimizing, and/or removing privacy impacts;
- unsatisfactory levels of accountability and/or oversight; and
- identification of when personal information is unnecessary to meet objectives.

A PIA can be separated into two stages.

Stage 1: The completion of a **privacy compliance checklist,** which analyzes what personal information is being collected. If the privacy compliance checklist leads to a determination that personal information is being collected, then the next stage must be undertaken.

Stage 2: The completion of a **comprehensive assessment** is only required if the privacy compliance checklist determines that personal information is being collected. If no personal information is involved, the second stage need not be undertaken.

The purpose of a PIA is to ensure that personal information is managed safely, securely and responsibly in accordance with legislative requirements. Its purpose is not to prevent information from being appropriately collected, used, retained and disclosed, but rather to ensure that appropriate operational practices are applied throughout the information lifecycle.

Why should a school board/authority do a PIA?

School board officials should consider conducting a PIA when they plan a new system or administrative practice or major changes to an existing system or practice that will collect, use and/or disclose personal information.

The PIA process is a due diligence exercise in which school boards can identify and address potential privacy risks that may occur in the course of their everyday operations.

A PIA is a valuable tool to provide review and feedback before a school board/authority implements proposed administrative practices and information systems relating to the collection, use, or disclosure of data/information identifying individuals.

A PIA may also be conducted when reviewing existing systems and practices for privacy compliance.

It is advisable for school boards to conduct a PIA in order to:

- confirm legal authority to collect, use, and disclose personal information;
- ensure fair information practices;
- identify and manage potential privacy risks through appropriate documentation (e.g., policies and procedures);
- communicate key messages and update notifications and privacy statements;
- save time and money (to avoid redesign or retrofit late in the development stage of an initiative or project);
- mitigate the risk of a privacy breach; and
- assure senior management that privacy policy and legislative compliance have been fulfilled.

A PIA is more than just a privacy compliance tool; it is an information management tool.

What are the major benefits for school boards/authorities of conducting a PIA?

- **Ensuring that individual privacy is protected**
  A PIA helps a school board determine if there are privacy risks associated with a particular program or service.
- **Promoting an awareness and understanding of privacy issues**
  A PIA puts privacy at the forefront of any new initiative.
- **Reducing the risk of non-compliance**
  A PIA helps school boards/authorities reduce the risk of non-compliance with privacy legislation and policies. This helps avoid costly redesigns of programs and services and assures student and employee stakeholders that their privacy is safeguarded.
- **Assisting school board officials to make better decisions**
  A PIA provides information to school board/authorities officials about privacy risks inherent in a new or redesigned program or service. Having this information helps these officials make better decisions.
- **Promoting trust and confidence**
  Public trust and confidence in the operations of a school board/authorities is increased by the knowledge that the PIA process is in regular and consistent use within the board.

A PIA has other benefits, including:

- identifying the potential for particular privacy impacts, such as additional uses of personal information that may evolve from the original stated uses and expectations or those that may arise from new legislation or technology;
- improving the project's consultation process, including public consultation (where necessary), so that privacy issues are more comprehensively identified and stakeholders are better informed;
- demonstrating to others that the handling of personal information in the project has been critically analyzed with privacy in mind; and
- playing a broader educational role about privacy, that can benefit not only the project, but also the board as a whole.

The information gathered in a PIA can also be used as part of the school board's/authority's broader project management processes for identifying risks to privacy.

A PIA helps to avoid costly and/or embarrassing privacy mistakes because it can:

- be used at the design stage to identify what needs to be done to ensure a project's compliance with privacy legislation and other board-specific or board-related legislative requirements-any necessary adjustments can be made during a project's development so that it will comply with all relevant laws that relate to the handling of personal information;
- include a list of applicable privacy laws and show the data-handling practices of the project, as well as the organizational rules to carry out these practices (e.g., policy and procedures), to comply with the specific provisions of the identified laws;

- provide an opportunity to consider community values (e.g., trust, respect, individual autonomy and accountability) and to reflect those values in the project by meeting the community's privacy protection expectations; and
- be used as a resource to broaden the school board's/authority's risk management processes in general.

A PIA can be a valuable tool to help identify what needs to be done to ensure a project's compliance with privacy legislation and/or other governing legislation.

What are the risks for school boards/authorities of not doing a PIA?

The risks associated with failing to appropriately address privacy issues can have an impact on the success of an initiative or project. These risks include:

- breach of an individual's personal privacy;
- failure to comply with relevant privacy legislation (i.e., breach of privacy);
- loss of credibility and trust of the community because of failure to meet expectations with regard to the protection of personal information (negative publicity); and
- systems redesign or retrofit late in the development stage (often at considerable expense).

How does an effective PIA work?

A PIA works most effectively when it is an integral stage/step of a project's design and development. By undertaking a PIA as an integral part of new projects, the school board/authority is able to:

- describe fully and systematically the way personal information "flows" in the project;
- analyze how these information flows will have an impact on privacy;
- identify the project's potential for further privacy risks;
- consider alternative privacy practices during project development rather than retrospectively; and
- make informed choices and recommendations about how the project will proceed.

A PIA is important in the development of a project involving personal information and should be an evolving or "living document." As the project develops and issues are identified, the PIA document can be updated and supplemented, resulting in the completion of a more comprehensive and useful PIA. A PIA should also be considered for existing projects.

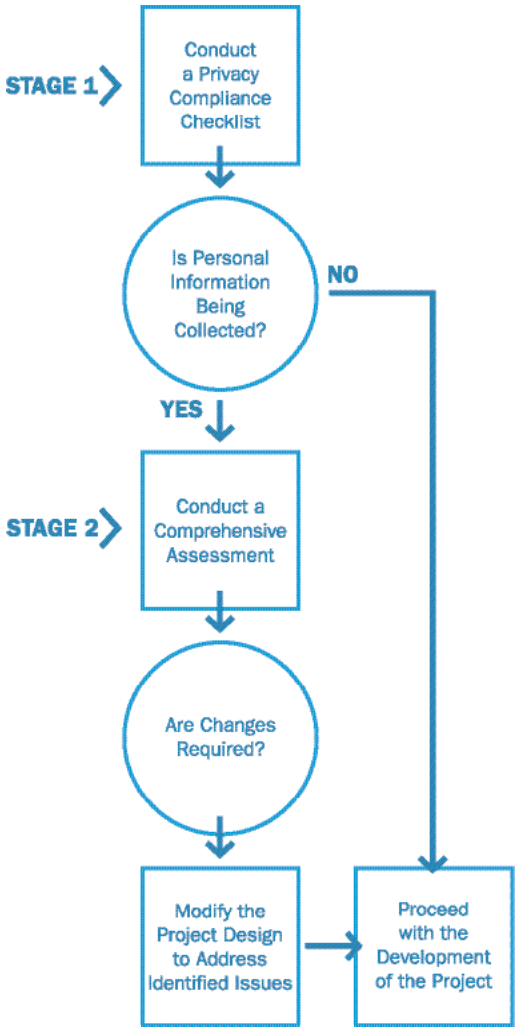
A PIA works best when it forms part of a project's evolution.

The stages of Privacy Impact Assessment

A PIA is comprised of two stages:

Stage 1: Privacy Compliance Checklist

Stage 2: Comprehensive Assessment



Privacy Compliance Checklist

A privacy compliance checklist (see Appendix C) is an important and useful first step in the PIA process. It should be completed for all new or redesigned projects, programs, technologies, initiatives, applications, and organizational practices. The checklist is a preliminary assessment of a project to identify the nature and sensitivity of any personal information that may be collected, used, or disclosed by the project, as well as the legal authority for the project/program.

Comprehensive Assessment

The comprehensive assessment (see Appendix D) is generally required for any project that:

- directly collects, uses or discloses personal information;
- indirectly collects personal information from any source;
- uses or expands the uses of common personal identifiers (e.g., OEN, MEN, SIN);
- introduces a new program or substantial system redesign of an existing program or system that collects, uses, or discloses personal information; or
- contracts with a third party to collect, use, or disclose personal information.

Once it is determined that personal information is involved in the project, the fundamental premise behind a comprehensive assessment is the mitigation of a potential privacy breach.

Understanding the purposes and function of a PIA will assist in deciding whether or not to implement a PIA for any given project. The primary driver is a substantial change in the collection, use, disclosure, or retention of personal information.

Planning the Comprehensive Assessment

Once the school board/authority has determined that a comprehensive assessment is necessary, the next consideration is the most appropriate design and approach based on the completed privacy compliance checklist.

Planning the most appropriate process will be influenced by the nature of the project. The design can be determined by looking at the project's:

Stage of development	Is it at the early or conceptual stages of development, or at a more advanced or detailed stage of development?
Scope	Is it limited or broad in scope?
Type	Is it a new program or system, or an alteration or "incremental" change to an existing program or system?
Personal information	Does it involve a limited or significant amount of personal information? What is the quantity and sensitivity of the personal information being handled?
Public impact	Does the project involve the handling of significant amounts of personal information about each individual, or the handling of personal information about a significant number of individuals? What is the public's perception of and expectation for the security of this personal information?
Interaction	What is the degree of interaction between personal information in more than one database (e.g., sharing or data-matching across the system, or across jurisdictions, or between the public and private sectors)?
Outsource	Will personal information handling be outsourced?

In general, the key components of a comprehensive assessment include the following:

Project description	Broadly describe the project, including the project's aims and whether any personal information will be handled.
Mapping the information flows	Describe and map the flows of personal information in the project.
Privacy impact analysis	Identify and analyze how the project impacts upon privacy.
Privacy management	Consider alternative options, particularly those that improve privacy outcomes while still achieving the project's goals.
Report and recommendations	Produce a final PIA report that includes the above information and recommendations.

Each of the above components should be addressed to some extent in every comprehensive assessment, with the level of detail being determined by the nature and stage of the project.

Who is involved in conducting a PIA?

Generally, a PIA uses a team approach and makes use of the various in-house experts available within the school board/authority, including staff responsible for access and privacy. It may consist of different stages and personnel as the project evolves. It is important to identify an individual or group of individuals who will be responsible for the completion of the PIA. The PIA leadership should have a clear mandate to review the project design decisions against the criteria of the PIA and provide the necessary advice and feedback to the senior project management team.

Some projects have considerably more privacy impact than others. In those cases, an independent PIA conducted by external privacy consultants or law firms may be preferable. Representation from school councils may also be advisable in some cases to provide input on the community's values and privacy protection expectations.

An individual staff member working in isolation would not undertake a PIA; it may consist of different stages and personnel as the project evolves. This "team" approach should be decided by assigned school board/authority individuals based on the scope of the project.

The following chart indicates who could be involved in a PIA and the types of skills they can provide:

PIA Leadership Role	PIA Leadership Skills
Project manager / team members	• Drive the process. • Build privacy component into the project plan. • Plan PIA activities in accordance with established project management principles.
Senior administration rep. (Superintendent)	• Support and advocate privacy commitment to approved project.
FOI Coordinator / privacy contact officer / records management	• Provide privacy expertise regarding standards, legislation, technologies and privacy developments. • Provide procedural and legal skills related to privacy and protection of recorded information.
Information technology	• Provide technology and systems expertise relating to the design and operation of the system/project application, networking products, Internet tools, system security, and front-end interface systems accessing the information.
Communications	• Document and publish essential notifications and information updates.
Other identified partners and stakeholders (e.g., students, parents, employees, ethics considerations) Σ	• Contribute to operational knowledge and understanding of the function of the project and the uses of the information. • Become familiar with the policies and procedures associated with the project, operational and business design skills related to the project.
Legal counsel/external consultants	• Provide legal and specialized expertise with regard to specific areas of the PIA or project, as required. This will be dependent upon the complexity of the personal information being assessed.

These roles are fundamental to ensuring that the PIA component of a project will be successful. Some individuals may play multiple roles, but it is important to assign the roles to specific individuals.

Why are consultation and transparency important to the PIA process?

Consultation, communication, and transparency are key to the success of any project that involves partners and/or significant stakeholders. A PIA is not just based on information technology. Business partners have to articulate the purpose. Privacy partners have to articulate the legislative and policy requirements. IT partners have to provide the technology context. Each contribution informs the assessment. Consultation with key stakeholders helps to ensure that key issues are noted, addressed, and communicated.

Similarly, wherever possible, publishing the contents and findings of a PIA can add value to the PIA and to the project. Publishing helps to demonstrate to stakeholders and the community that the project has been critically analyzed with privacy in mind. Publishing also represents good practice by contributing to the transparency of the project.

Where warranted, a PIA that incorporates public consultation can also help to garner broad community awareness and confidence in the project.

The PIA process is designed to ensure that privacy is considered throughout the business redesign or project development cycle, and particularly at the conceptual stage, the final design approval and funding stage, the implementation and communications stage, and the post-implementation audit or review stage.

DOING THE PIA

Overview of the Process

The PIA process requires a thorough analysis of potential impacts on privacy and a consideration of measures to mitigate or eliminate any such impacts. The privacy impact assessment is a due diligence exercise in which the organization identifies and addresses potential privacy risks that may occur in the course of its operations.

While PIA's are focused on specific projects, the process should include an examination of organization-wide practices that could have an impact on privacy. The school board's/authority's privacy policy and procedures, or the lack of them, can be a significant factor in the ability of the school board/authority to ensure that privacy protection measures are available for specific projects.

The onus always remains on the Board to ensure adequate levels of privacy protection, as required in applicable legislation MFIPPA or PHIPA, and if challenged in this regard, the Privacy Commissioner's Office will look for proof that the Board has made reasonable efforts to protect privacy. A PIA cannot be used to obtain a waiver of, or release from, any requirement of the relevant legislation.

A PIA is a process that helps to determine whether new technologies, information systems, and proposed programs or policies meet basic privacy requirements. It also measures both technical compliance with privacy legislation, such as the MFIPPA and PHIPA, and the broader privacy implications of a given proposal. The PIA is also intended to help policy writers and decision-makers manage potential privacy risks.

As noted in sections 1.1 and 2.0, the two stages of the PIA process are:

1. **Conduct a Privacy Compliance Checklist**
   i. If it is determined that no personal information is being collected, the project may proceed.
   ii. If it is determined that personal information is being collected, proceed to Stage 2.
2. **Complete a Comprehensive Assessment**
   i. If it is deemed that changes are required with regard to the way personal information is collected, used, disclosed or secured for compliance with the *Ontario School Board Privacy Standard*, the project design must be modified to address these issues before it can proceed.

The end result of the PIA process is documented assurance that all privacy issues have been appropriately identified and adequately addressed or, in the case of outstanding issues, brought forward to senior management for further direction.

Privacy Impact Analysis – Privacy Compliance Checklist

In order to provide assurances that all relevant factors and potential privacy issues have been addressed, the following four key areas must be considered in the process:

1. *People* are important for two reasons: first, they handle personal information and must be aware of how that information is collected, used, retained and disclosed; second, as part of the privacy compliance environment, they must create and monitor the effectiveness of policies and processes. Privacy policies set boundaries and establish the privacy rights and obligations of parties.

   Consider: Ongoing management, privacy training programs, general organizational awareness of privacy and security issues, the level of knowledge required to perform specific functions, and the availability of manuals and other forms of guidance and/or mechanisms for communicating privacy and security policies and procedures.

2. *Processes* are necessary to implement the policies and procedures and are designed to ensure that a consistent message is communicated throughout the organization.

   Consider: What information is collected, why and how it is collected, how privacy and security are ensured operationally, and what mechanisms are in place to provide individual access to information.

3. *Systems* provide a means of protecting personal information through a variety of physical and electronic controls and other security measures.

   Consider: System design characteristics, data security and integrity measures, authority, access controls, and audit trails.

4. *Records management practices* establish a framework within which personal information is managed.

   Consider: The physical space where information is stored, physical security measures, the availability of secure document disposal facilities, and processes for secure disposal of old information technology, encryption technology, password protection, levels of authority (e.g., personal computers, legacy servers, etc.) which may hold personal information.

The PIA investigates how the flow of information in a project affects the choices individuals have regarding how personal information is handled, the intrusiveness into the private lives of individuals, the compliance with privacy law, and how the project fits into community expectations.

The Privacy Impact Analysis should consider:

- *which privacy impacts are serious and which are less so;*
- *whether the privacy impacts are necessary or avoidable; and*
- *how the privacy impacts may affect the broad goals of the project.*

Key questions to be answered through the privacy impact analysis phase of a PIA can be determined by conducting a Privacy Compliance Checklist (see Appendix A). This questionnaire investigates whether the personal information aspects of the project comply with applicable privacy laws.

Ontario School Board Privacy Standard – Comprehensive Assessment

The *Ontario School Board Privacy Standard* is a commitment we are applying in the collection, use and disclosure of personal information/data and addressing issues of privacy, security and confidentiality. These privacy commitments are based on the *Model Code for the Protection of Personal Information* that was developed by the Canadian Standards Association and was recognized as a national standard in 1996.

The Ontario School Board Privacy Standard can also be used for discussion purposes to complete a Comprehensive PIA (see Appendix B).

The ten commitments, with explanatory notes, are as follows:

1. **Accountability and Responsibility:** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles

Start by identifying internally who will be your privacy officer(s). Such individuals must be designated by the school board/authority. As personal Information may be collected and processed by different departments within your organization, you should also consider whether a team of individuals would be necessary to ensure the whole board is compliant with the Act.

2. **Specified Purposes:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Conduct a "privacy audit" to determine what personal information you collect and for what purpose. Check your forms and publications and/or websites to ensure privacy statements that identify purpose for collection of personal information are present and visible where necessary. It is also important to ensure the availability of other information that may be required by law (i.e., legal authority for collection, and the title, business address, and telephone number of a person who can respond to questions about collection). Contact information for your privacy officer(s) should also be easily accessible.

3. **Consent:** The knowledge or consent of the individual is required for the collection, use, or disclosure of personal information, except when not required by law.

Consent is generally not necessary under MFIPPA, except in limited cases where information is being collected indirectly. However, this does not mean that consent cannot form part of the collection process. As part of your audit, consider how you collect information. As varying types of consent are possible, consider which is most appropriate to the nature, including sensitivity, of the information you collect.

4. **Limiting Collection:** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

This means that an organization must limit the type of information collected to correspond with the stated purpose. Section 28(2) of MFIPPA provides that "no person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity." Sections 29(1) and (2) of MFIPPA outline the manner of collection and notice requirements to the individual regarding the collection of personal information, including the principal purpose or purposes for which the personal information is intended to be used.

5. **Limiting Use, Retention, and Disclosure:**Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes, or as required by law.

Your privacy policy must include guidelines that govern the handling of personal information while your organization is using it, including minimum and maximum times for retaining it. Information used to make a decision about an individual should also be kept long enough to allow the individual to have access to it.Section 30(1) and (4) of MFIPPA ensures that personal information must be collected, used, disclosed, retained and disposed of in accordance with the regulations. (O.Reg. 823/90) Note: MFIPPA contains minimum but not maximum retention periods.

6. **Accuracy:** Personal information shall be as accurate, complete, and up-to-date as necessary for the purposes for which it is to be used.

Under sections 30(2) and 30(3) of MFIPPA, institutions must take reasonable steps to ensure that personal information within the records of the institution is not used unless it is accurate and up-to-date, with the exception of personal information that is prohibited by legislation for routine updating if it is not necessary to fulfill the purpose given for the initial collection, e.g., law enforcement purposes.

7. **Security Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

As part of your procedures identify methods of secure storage and disposal. Such procedures can include physical and technical measures as needed, as well as staff education and awareness.

8. **Openness and Transparency:** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Specific information about personal information policies and practices must be readily available in an understandable form. This must include the name or title and address of the privacy officer and a description of the type of personal information the school board/authority collects, uses, and retains. Under sections 25 and 34 of MFIPPA, institutions must make available a Directory of General Records and Personal Information Banks for inspection by the general public or for clarification by a requester seeking access to records and information under the care, custody, and control of the institution and is required to document specific information about such banks.

9. **Access and Correction:** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Under sections 36 and 37 of MFIPPA, every individual has a right of access to personal information that is in the custody or under control of an institution, with specific exemptions as noted under section 38 of MFIPPA. In addition, every individual who is given access to his/her personal information is entitled to ensure that the information is accurate and complete and, if it is not, to request that it be corrected, or to have a statement of disagreement attached to the personal information that was not corrected as requested.

10. **Compliance:** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's privacy compliance.

The school board/authority must be ready to respond to privacy complaints, including amending policies and practices if necessary. School boards/authorities must also be ready for compliance audits and appeals relative to the access to and/or release of personal information, should there be reasonable grounds to believe that the organization has acted in contravention of the Act(s). The Office of the Information and Privacy Commissioner/Ontario will investigate these matters.

In practice, organizations (including school boards/authorities of education) can use the ten commitments of the Privacy Standard in developing a privacy policy.

The Privacy Standard can also be used to develop a comprehensive PIA.

Report and Recommendations (see Appendix C: Privacy Impact Assessment Report)

The Assessment Has Been Done... What's Next?

The PIA report with its findings and recommendations is a valuable resource, assisting the project team, senior management, and other stakeholders. The PIA can be used to further inform and educate those involved in, or affected by, the project.

For example:

- The PIA should feed into further planning about the project's next steps. This may include resource allocation; stakeholder management; advising the senior management and governing body (the board) about risks; staffing; designing; piloting; testing; consultation; public education; and evaluation;
- Generally, PIA findings should be published at the appropriate stage, in particular to ensure that key stakeholders have a copy; and
- PIA findings may need to be revisited at different phases or for different aspects of the project as it progresses.

Documentation of the PIA investigation, analysis, assessment, and findings forms an ongoing, useful decision-making tool for the organization. Providing a PIA report also enables the success of any PIA recommendations implemented to be reviewed as part of the post-implementation review of the project.

Organizations are encouraged to include the PIA findings during any subsequent public consultation on the project. Organizations are also encouraged to make the PIA findings available to the public as part of the project's implementation.

Privacy and project goals can both be achieved.

Acknowledgements and References

Government of Ontario (June 2001). Privacy Impact Assessment: A User's Guide. Information and Privacy Office; I & IT Strategy; Policy, Planning and Management Branch. Officer of the Corporate Chief Strategist, Management Board Secretariat.

Information Privacy Commissioner (October 2005). *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act.*

Office of the Information and Privacy Commissioner (January 2001). *Privacy Impact Assessment: Instructions and Annotated Questionnaire.* Alberta, Canada.

Office of the Privacy Commissioner (August 2006). *Privacy Impact Assessment Guide: Australian Government.*

Related Links

Ontario Ministry of Government Services, Privacy Impact Assessment Guidelines
http://www.accessandprivacy.gov.on.ca/english/pia/pia.html

PIA Compliance Checklist

		Yes	No	Don't Know
1a	Does the project collect, use or disclose any amount of personal information about identifiable individuals? (e.g., OEN, MEN, DOB, SIN, OHIP, employee number, telephone number and address) MFIPPA 29(1), (2), 28(2), 31, 32, 33	☐	☐	☐
1b	Has the legal authority for the collection, use and disclosure of all personal information for this project been established (e.g., Education Act, OSR Guidelines, MFIPPA, Income Tax Act, Occupational Health and Safety Act, Employment Standards Act)? Provide relevant reference and/or documentation for compliance with the appropriate legislation.	☐	☐	☐
1c	Does individual consent provide the primary authority for the collection, use and disclosure of personal information for this project? If individual consent does NOT form the basis for the collection, use and disclosure of personal information, please identify the alternative authority that applies (e.g., no consent necessary for direct collection under MFIPPA). This may be cross-referenced with question 1(b) above (e.g., admissions/assessment information). Please provide any documentation that clearly sets out the purposes for which personal information will be collected.	☐	☐	☐
1d	Have the purposes for which the personal information is collected been determined and documented (e.g., student registration, employment purposes)? Do the data collection documents meet the requirements for providing legal notice? MFIPPA s.29(2)	☐	☐	☐
1e	Will personal information be used exclusively for the identified purposes and/or for uses that an individual would reasonably consider consistent with those purposes (e.g., sharing of student achievement data for research purposes, which should be limited and exclusive)? If not, does the law permit other uses? MFIPPA s.31 and 32	☐	☐	☐
2	Does the project create entirely new identifiers to provide access to personal information about specific individuals?	☐	☐	☐
3	Does the project consolidate, interlink, cross reference, or match personal information from multiple sources? (e.g., data warehouse, class portal)	☐	☐	☐
4	Does the project expand existing services, programs or technologies which collect personal information, such that they require the sharing or dissemination of personal information among other institutions? (e.g., transportation consortia)	☐	☐	☐

PIA Compliance Checklist

		Yes	No	Don't Know
5a	Does the project expand existing services, programs, or technologies that collect personal information such that they require the sharing or dissemination of personal information to third party organizations that are adherent to (or governed by) MFIPPA, FIPPA, PHIPA or comparable privacy protection (e.g., district health units, faculties of education, Ministry of Community and Social Services)? **MFIPPA 14(1) (e) (iii), PHIPPA 10(4)**	☐	☐	☐
5b	Does the project require the outsourcing of information management functions to third party organizations that are adherent to (or governed by) MFIPPA, FIPPA, PHIPA or comparable privacy protection (e.g., legal counsel, security services, or achievement software such as Media-X's MXWeb product, which can be housed on Media-X's servers or may involve sharing a copy of our student systems database with the vendor to assist in troubleshooting a problem that the vendor is unable to replicate in-house)?	☐	☐	☐
6a	Does the project expand existing services, programs, or technologies that collect personal information such that they require the sharing or dissemination of personal information to third party organizations that are not adherent to (or not governed by) MFIPPA, FIPPA, PHIPA or comparable privacy protection?	☐	☐	☐
6b	Does the project require the outsourcing of information management functions to third party organizations that are not adherent to (or not governed by) MFIPPA, FIPPA, PHIPA or comparable privacy protection (e.g., payroll)?	☐	☐	☐
7	Does the project span multiple jurisdictions or multiple government institutions or otherwise involve a high degree of organizational complexity, with the potential of data sharing (e.g., OnSIS, consortia, EDI or other partnerships)?	☐	☐	☐
8	Does the project involve the disclosure of personal information outside Ontario or the exchange of personal information with organizations that have head offices outside Canada (including project vendors, contractors, partners and others)?	☐	☐	☐

		Yes	No	N/A	Don't Know
	Commitment 1: Accountability and Responsibility				
P1-1	Is there a person designated who is accountable for privacy protection and compliance?	☐	☐	☐	☐
P1-2	Are there clearly defined responsibilities and accountabilities for safeguards to protect personal information?	☐	☐	☐	☐
P1-3	Is there a written policy or statement of information practices?	☐	☐	☐	☐
P1-4	Have privacy policies or procedures been developed?	☐	☐	☐	☐
P1-5	Is there a process in place to regularly review privacy policies and procedures?	☐	☐	☐	☐
P1-6	Does a reporting process exist to ensure that senior management is informed of any privacy compliance concerns?	☐	☐	☐	☐
P1-7a	Is personal student or staff information collected, used, or disclosed to third party partners in carrying out programs or services on behalf of the school board/authority?	☐	☐	☐	☐
P1-7b	If yes, are provisions in place to ensure that the third party meets the school board's/authority's privacy protection requirements (e.g., software vendor agreements, purchasing agreements, data sharing agreements)?	☐	☐	☐	☐
	Commitment 2: Specified Purposes				
P2-1	Has the purpose for collecting personal information been identified in relation to the program's functional and operational requirements?	☐	☐	☐	☐
P2-2	Does the notice of collection identify ALL of the following: • a description of the personal information to be collected? • the legal authority for its collection? • the principal purpose(s) for which it is collected? • the name, position, address and telephone number of a contact person? **MFIPPA 29(2)**	☐	☐	☐	☐
P2-3	If there are secondary purposes that are not included in the notice of collection, have these been documented elsewhere, such as in the Directory of Records, or attached to the record (e.g., audit trail information, OnSIS transaction validation, professional development materials, financial settlements)? **MFIPPA 25 (1)b, 34 (1) a-g, 35 (1) a, b**	☐	☐	☐	☐

		Yes	No	N/A	Don't Know
P2-4	Is client notification sent for secondary uses of personal information, such as longitudinal tracking, service monitoring, and program evaluation?	☐	☐	☐	☐
P2-5	Do all forms, pamphlets, websites, and information collection and disclosure instruments clearly state the purpose(s) for the collection, use, and disclosure of personal information?	☐	☐	☐	☐
P2-6	Is the notice of collection available to all persons affected, regardless of the medium or service channel they use?	☐	☐	☐	☐
P2-7	Are there procedures to periodically review the purposes for personal information collected?	☐	☐	☐	☐
	Commitment 3: Consent				
P3-1	Is there a requirement that an individual's consent be obtained before or at the time personal information about the individual is collected and before any new use or new disclosure of the information, or is notice sufficient? **MFIPPA 29(1), 31a-c, 32**	☐	☐	☐	☐
P3-2	Where consent is necessary (e.g., for indirect collection), are individuals informed of the consequences for not providing consent?	☐	☐	☐	☐
P3-3	Are individuals advised that they can alter or withdraw consent (where permitted) after it is granted?	☐	☐	☐	☐
P3-4a	Has the purpose for collecting personal information been identified in relation to the program's functional and operational requirements?	☐	☐	☐	☐
P3-4a	Does the project envision possible secondary uses for the personal information collected? **MFIPPA 31 a, b, c**	☐	☐	☐	☐
P3-4b	If yes, does the authority for those uses flow from the initial notice of collection (i.e., is it for a consistent purpose), or is the use by an officer, employee, agent, or consultant of the board who need the information in the performance of his/her duties where use is necessary and proper to the discharge of board functions (e.g., effective educational program planning, appropriate resource allocation, advocacy for resources, funding from external partners to support students) or some other authority (e.g., disclosure to law enforcement agency for a criminal investigation)?	☐	☐	☐	☐
P3-5	Are individuals informed that they are allowed to restrict or limit the disclosure of their personal information where appropriate and feasible?	☐	☐	☐	☐

		Yes	No	N/A	Don't Know
	Commitment 4: Limiting Collection				
P4-1	Is the collection of personal information limited to that which is needed for the identified purpose(s)?	☐	☐	☐	☐
P4-2	Is the collection of personal information: • authorized by statute? • necessary for the proper administration of a lawfully authorized activity? **MFIPPA 28(2)**	☐	☐	☐	☐
P4-3	Is personal information collected directly from the individual? **MFIPPA 29(1), 31 a-c, 32**	☐	☐	☐	☐
	Commitment 5: Limiting Use, Retention, and Disclosure				
P5-1	Is personal information used only for the stated purposes or for uses that are consistent with those purposes? If not, are other uses permitted by law? **MFIPPA 31(b)**	☐	☐	☐	☐
P5-2	Has the unnecessary linkage of personal information across multiple databases been avoided?	☐	☐	☐	☐
P5-3	If no, is that linkage performed only with internal identifiers instead of widely used identifiers such as the OEN, MEN or social insurance number?	☐	☐	☐	☐
P5-4	Is there a timetable for retaining and disposing of personal information? Have any minimum and/or maximum retention periods been considered?	☐	☐	☐	☐
P5-5	When personal information is no longer required for the identified purpose(s), or it is no longer required by law, is it destroyed, erased, or depersonalized?	☐	☐	☐	☐
	Commitment 6: Accuracy				
P6-1	Do personal information files: • record the date when the information was obtained or updated? • specify when and how the information is to be updated and the source for the update? • indicate how to verify the accuracy and completeness of information disclosed to or received from a third party?	☐	☐	☐	☐
P6-2	Is there a procedure to provide notices of correction to third parties to whom personal information has been disclosed? **MFIPPA 36(2)(c)**	☐	☐	☐	☐
P6-3	Are there records kept regarding requests for a review for accuracy, corrections, or decisions not to correct? **MFIPPA 30(2)**	☐	☐	☐	☐

		Yes	No	N/A	Don't Know
P6-4	If the individual and the school board representative cannot reach agreement regarding the accuracy of the record(s), is the individual advised of his or her right to file a statement of disagreement? **MFIPPA 36(2)(b)**	☐	☐	☐	☐
P6-5	Does the custodian of the record note the statement of disagreement on the record(s) in such a manner as to ensure that subsequent users who access the record(s) through any service channel are aware that the accuracy of the record(s) is disputed? **MFIPPA 36(2)(b)**	☐	☐	☐	☐
P6-6	Are there periodic reviews to check the accuracy of personal information records and to correct them as necessary to minimize the use of inappropriate data for decision making? **MFIPPA 36(2)(b)**	☐	☐	☐	☐
	Commitment 7: Security Safeguards				
P7-1	Do written security policies and procedures exist to protect the privacy, integrity, and availability of personal information, or will they exist before the project is completed? **MFIPPA 34(1)(g)**	☐	☐	☐	☐
P7-2	Are staff or agents with access to personal information provided with privacy training?	☐	☐	☐	☐
P7-3	Are procedures in place to revoke access privileges and recover security tokens and keys when employment is terminated or when job functions change (e.g., through transfer or promotion)?	☐	☐	☐	☐
P7-4	Are procedures in place to address incident reporting and investigation procedures?	☐	☐	☐	☐
P7-5	Are policies and procedures in place to handle privacy breaches, including the notification of individuals when the security or privacy of personal health information has been breached, if required?	☐	☐	☐	☐
P7-6	Are there controls in place over the process to grant authorization to add, change, or delete information from records?	☐	☐	☐	☐
P7-7	Is the system designed so that access and changes to personal information can be audited by date and by user identification?	☐	☐	☐	☐
P7-8	Do contracts with business partners specify privacy and security requirements and expectations with respect to personal information?	☐	☐	☐	☐
P7-9	Are there processes in place to confirm that business partners are complying with privacy and security requirements?	☐	☐	☐	☐

		Yes	No	N/A	Don't Know
P7-10	Is sensitive information labelled, transmitted, and stored in accordance with existing information security and privacy policies and procedures?	☐	☐	☐	☐
P7-11	Are policies and procedures in place for archiving of data, e-mail, and both hard copy and electronic documents?	☐	☐	☐	☐
P7-12	Is personal information disposed of under secure conditions?	☐	☐	☐	☐
P7-13	Are security measures in place for the disposal of equipment such as computers, diskettes, and filing cabinets that may have personal information stored within them?	☐	☐	☐	☐
P7-14	Are disaster recovery and business continuity plans in place for all mission-critical organizational processes?	☐	☐	☐	☐
P7-15	Has a threat-risk assessment been completed in conjunction with the project?	☐	☐	☐	☐
	Commitment 8: Openness and Transparency				
P8-1a	Have written policies and procedures regarding the management of personal information been developed?	☐	☐	☐	☐
P8-1b	If yes, have they been communicated to staff, parents and students?	☐	☐	☐	☐
P8-2	Is the privacy policy prominently displayed on the school board/ authority website?	☐	☐	☐	☐
P8-3	Are personal information policies and procedures clearly explained on documents used to collect personal information?	☐	☐	☐	☐
P8-4	Do privacy policies and procedures explain how to: • access personal information? • correct personal information? • make an inquiry or complaint?	☐	☐	☐	☐
	Commitment 9: Access and Correction				
P9-1	Are there policies and procedures for responding to access requests?	☐	☐	☐	☐
P9-2	Does the individual have access to his or her records of personal information and records related to requests for review or correction? **MFIPPA 36(1), 36(2)a**	☐	☐	☐	☐

		Yes	No	N/A	Don't Know
P9-3	Are there procedures in place: • to verify the identity of individuals requesting access to their information? • to facilitate a response to requests for personal information including those in alternate formats, such as Braille or audio tapes? • for correcting personal information if the individual requests, or annotating the information if a correction is not made? • to enable third parties that have received personal information for which a correction is requested to be notified? **MFIPPA 36(2)(c)**	☐	☐	☐	☐
P9-4	When access is limited or denied, are individuals advised in writing of the reasons for refusal and of any recourse available?	☐	☐	☐	☐
	Commitment 10: Compliance				
P10-1	Can an individual easily find out how to file a privacy complaint related to the project?	☐	☐	☐	☐
P10-2	If a complaint is justified, is inaccurate personal information corrected and policies and procedures amended accordingly?	☐	☐	☐	☐
P10-3	Are individuals informed that a statement of disagreement can be included with their personal information when an amendment to their information is not allowed? **MFIPPA 36(2)a**	☐	☐	☐	☐
P10-4	Are individuals advised of their right, where applicable, to complain to the Information and Privacy Commissioner? **MFIPPA 39(1)**	☐	☐	☐	☐

Adapted from the Ministry of Government Services (MGS) PIA guidelines

Project Name:	
Version:	
Date:	
Author:	

Document Approval:

Name	Title	Date

Project Background

Describe the project that is being assessed, its purpose, time frames, delivery mechanisms, and other information relevant to its management of personal information.

Project Description:

Executive Summary

In laypersons' terms, provide a brief summary of the project and the findings of the PIA. The Executive Summary should highlight major findings, identified problems, and proposed solutions or recommendations to reduce risk.

Major PIA Findings	Identified Privacy Problems	Recommendations to Reduce Risk

Introduction

Rationale for PIA:
Project Objectives:
Scope of the PIA (define the boundaries of the project):

Legislative and Policy Authorities for The Project

Where personal information is collected/used/disclosed by an institution, the institution must demonstrate that the collection, use and disclosure is in accordance with the *Education Act, MFIPPA/PHIPA.*

Description of Personal Information

No PIA is complete unless it identifies all personal information associated with the project and a recording of the information flow and business process model for linking, storage, and disposal of data records.

Personal Information Listing (Name, address, OEN, MEN, birth date, aboriginal status, etc.):

Data Flow Description and Maps (Data flow documentation depicts data flows into and out of the responsible entity. It concentrates on personal student and/or employee information collection, use and disclosure. Business process diagrams are a useful adjunct to the data flow documentation. Possible approaches to mapping the business process would include flow charts and business process models):

Potential Privacy Risks

Identifies the major privacy issues that the project might encounter and how best to minimize them.

Overview of Security and Monitoring Requirements

The PIA should include a discussion of the methods that will be used to monitor privacy compliance and secure data integrity throughout the project life cycle.

PURPOSE

This glossary is designed for use in school boards/authorities in the Province of Ontario and draws on nationally and internationally recognized sources of best practice. The glossary is not a comprehensive listing of all terms used in records management. Terms chosen are those used in Ontario school boards/authorities and the definitions reflect this usage.

Access	Authority or permission to consult records or to obtain restricted information.
Access Control	A set of rules or policies that dictate each user's access rights to particular information in an organization.
Active Records	Documents or records required for day-to-day business relating to the administration or function of the organization. Active records are normally referred to more than once per month. Also referred to as current records.
Analogue Record	A record in a non-paper format that is still readable by the human eye without the aid of a computing device.
Application	A collection of one or more related software programs that enables a user to enter, store, view, modify, or extract information from files or databases.
Appraisal of Records	Determination of the value of records before their disposal. This evaluation is based on their current administrative, fiscal, and legal use, and on their value as evidence or as an information source.
Archival Records/Data	Information considered permanently valuable and preserved for reference and research purposes because it reflects significant events or documents the history and development of the organization. *See also: Permanent Records*
Archival Value	The permanent and continuing worth of records based on their administrative, legal, financial, or historical usefulness. Also called continuing value, enduring value, or historical value. Also referred to as enduring value.
Archive	To make a back up copy of a computer file for security. To store documents (records) for the purpose of later or long-term reference.
Archives	A repository for records with continuing value. *See Also: Remote Storage*
Authenticate	To verify the identify of a user, user device, or other entity. Authentication is the process of determining whether someone or something is in fact who or what it is declared to be.
Authenticity	Characteristic of a document or record created by the entity represented as its creator, and preserved in its original form without any falsification or tampering. A genuine signature is usually the best proof of authenticity.
Authentic Record/Document	A document or record that actually is what it says it is or is represented to be and is completely free of any addition, deletion, or corruption.

Backup Data	Data that is copied (backed up) onto secondary media for purposes of offline, off-site security storage. The primary purpose of data backup is to provide the capability of recovering critical when a data loss of any kind occurs.
Breach (Privacy Breach)	An infraction or violation.
Business Management Practice	The ongoing management of all business processes for an organization, including the development, alignment, and continuous review of processes in support of the organization's goals.
Canadian Standards Association (CSA)	A not-for-profit, membership-based association serving business, industry, government, and consumers in Canada and the global marketplace to develop standards that address real needs, such as enhancing public safety and health.
Classification	The process of identifying records and information in accordance with a predetermined filing system. This includes determination of the function and/or subject of a record and selection of an appropriate classification for filing.
Classification System	A tool for organizing and filing records and documents based upon function and subject, for the purpose of facilitating filing and retrieval.
Comprehensive Assessment	A detailed analysis/review to assist school boards in determining the effects of a program or service delivery initiative on individual privacy.
Confidential Record	A record containing certain information that requires protection against unauthorized access or disclosure.
Conversion of Records Format	The transfer of recorded information from one physical medium or format to another. Conversion includes changing paper records to electronic format, and conversely, transferring records in electronic format to paper.
Data	Individual facts or values not significant to an organization until analyzed and/or preserved as a record of the organization's transactions and operations. Data on its own has no meaning; only when interpreted by some kind of data processing system does it take on meaning and become information.
Data Holding	An organized collection of information and data, either paper or electronic (e.g.,student information system, data warehouse, records room); a "holding" area for information.
Data Warehouse	A repository of an organization's electronically stored data.
Data Warehousing	The linking of all organization databases to a single relational database for the purpose of sharing information.
Date of Birth (DOB)	The hour (and minute), day, month, and year of birth established in order that exact age may be determined in completed years, months, days, and hours (and minutes) of life as required.
Destruction of Records	The various methods of destroying inactive records scheduled for destruction when authorized by shredding, incineration, pulping, or recycling. Methods for secure destruction of electronic records are also covered by this term.

Digital Record	*See: Electronic Document*
Disaster Recovery	The process of regaining access to (paper or electronic), hardware and software necessary to resume critical business operations after a natural or human-caused disaster. A disaster recovery plan (DRP) should also include plans for coping with the unexpected or sudden loss of key personnel responsible for any managed information.
Disposal	The final removal-whether for destruction or formal transfer to another agency, records storage centre or archives-of records that have reached the end of their retention period.
Disposition	Disposition refers to the finalizing activities that inactive records undergo. Includes storage, destruction by deleting an electronic record, and shredding/recycling of paper records.
Document	The smallest unit of filing housed in a filing system. Recorded information that (regardless of medium, form, or characteristics) serves to establish one or several facts and/or can be relied upon as a proof thereof.
Document Imaging	Microfilming or digitization of paper documents for easy storage, retrieval, and distribution.
Document Management Software	Software application used for managing documents that allows users to store, retrieve, and share them with the benefit of security and version control.
Document Management	Coordination and control of the flow (storage, retrieval, processing, printing, routing, and distribution) of electronic and paper documents in a secure and efficient manner in order to ensure that they are accessible to authorized personnel as and when required. *See also: Records Management*
Education Act	In Ontario, education is governed principally by the Education Act and its regulations. The Education Act and its regulations set out the duties and responsibilities of the Minister of Education and of school boards, school board supervisory officers, principals, teachers, parents, and students.
Electromagnetic Degaussing	Electromagnetic Degaussing A method of erasing or destroying data stored in magnetic media, such as hard drives, floppy disks, and magnetic tape using a strong magnetic field.
Electronic Data Interchange (EDI)	Represents the computer-to-computer transfer of information in a structured, predetermined format between two or more partners over a secured network.
Electronic Document	Information recorded in a manner that requires a computer or other electronic device to display, interpret, and process it. *See also: Electronic Record*
Electronic Document and Records Management System (EDMS)	Software that provides for the management of electronic documents in a variety of forms and formats using computer equipment and software to manage, control, locate, and retrieve information in the system. EDMS systems are designed to capture, route, and organize electronic documents. Many of these systems also provide document collaboration, revision/version control, secure access, and other features.
Electronic Imaging	Technology or process that records documents as digitized images on computer storage media for subsequent retrieval and use.

Electronic Record	Information captured through electronic means, and which may or may not have a paper record to back it up. *See also: Electronic Document*
Electronic Storage Media	Any device that is used to store or record electronic information, including, but not limited to hard disks, magnetic tapes, compact discs, videotapes, audiotapes, handheld electronic devices, and removable storage devices such as floppy disks and zip disks.
External Agencies	Organizations (other institutions, e.g., non-profit or not-for-profit) with which school boards share operations, information, and services.
Freedom of Information and Protection of Privacy Act (FIPPA)	The purpose of this Act is to provide the public a right of access to information subject to limited exemptions, and to protect the privacy of individuals with respect to personal information about themselves, as well as to provide individuals with a right of access to that information.
Forms Management	Establishing standards for the research, analysis, design (including format), production, and distribution of all forms used within an organization.
Functional Responsibility (Also called Office of the Record or Originator)	Certain sites are responsible for certain records and they are responsible for keeping those records for the full period of retention. These sites are responsible for the function or process that requires information from the records and/or generates the records.
Guideline	A recommended course of action.
Identity	The collective aspect of the set of characteristics by which a person is definitively recognizable or known.
Inactive Records	Documents no longer required in the day to day operations of an organization, but which must be kept for administrative, historical, fiscal, audit, or legal purposes.
Information	Organized data that has been arranged for better comprehension or understanding.
Information Management Standard	The systematic management and control of school board/authority information assets throughout its life cycle, which covers acquisition; receipt; creation; active use; maintenance; off-site storage; inactive use and preservation; and disposition, destruction, and transfer.
Information and Privacy Commissioner	A commissioner that acts independently of government to uphold and promote open government and the protection of personal privacy in Ontario.
Informed Consent	Informed Consent Requires that the person consenting understand the exact nature of the information for which consent is sought, understand the potential consequences of signing the consent form, and be given the right to revoke the consent at any time. Students 16 or older must sign the consent form. If a student is less than 16 years of age, parent or guardian must provide informed consent.
Lifecycle of a Record	The lifespan or time period from the creation or receipt of a record through to its final disposition. The five stages in the life cycle of a record include creation; distribution and use; storage or maintenance; retention and disposition; and archival preservation or ultimate destruction.
Managing Information for Student Achievement (MiSA)	A large-scale provincial initiative to increase provincial, district, and school capacities to work with data and information to support improved student achievement.

Memorabilia	Individual items of historical value such as programs, posters, brochures, clippings, photographs, etc.
Metadata	Data that describes the context, content, and structure of records and their management through time. An integral component of an electronic record, metadata describes (among other attributes) how, when, and by whom the record was collected, created, accessed, modified, formatted, and transferred.
Migration	The transfer of electronic records/data across hardware and software configurations and across subsequent generations of computer technologies, preserving its integrity. Used to ensure continued access to information as systems or media become obsolete overtime.
Ministry Educators Number (MEN)	Ministry Educator Number is assigned to an educator in Ontario. The number, which is unique to every educator, is assigned for life.
Municipal Freedom of Information and Privacy Protection Act (MFIPPA)	The provincial legislation that governs access to information and protection of personal information for municipal entities such as school boards, police services, and cities and towns.
Non-Record	A document such as a draft, worksheet, routine memo, or extra copy created for convenience or distribution, and which has no retention value and no need to be filed.
Office of the Record	The office assigned responsibility for custody and maintenance of specific records. Generally, the office in which they were originally created and filed. *See also: Functional Responsibility*
Official Record	A significant, vital, or important record having the legally recognized and enforceable quality of establishing a fact, and of continuing value to be protected, managed, and retained according to established retention schedule; often, but not necessarily, an original.
Ontario Association of School Business Officials (OASBO)	An organization of professionals that works collaboratively to support learning by developing and promoting excellence in business practices.
Ontario Education Number (OEN)	The OEN is a student identification number that is assigned by the Ministry of Education to elementary and secondary students across the province. The number, which is unique to every student, is used as the key identifier on a student's school records, and follows the student through his or her elementary and secondary education.
Ontario Health Insurance Plan (OHIP)	Covers the fees associated with health care services for Ontario residents that have a health card.
Ontario School Information System (OnSIS)	A web-enabled data collection system that was implemented as part of the MISA initiative.
Ontario Student Record (OSR)	The record of a student's educational progress through schools in Ontario.
Original Record	A primary or first-generation record from which copies can be made.
Organizational Taxonomy	A hierarchical structure for documents and information of major and subordinate categories from the most general to the most specific ; can be departmental, organizational, or functional.

Outsourcing	The process of subcontracting to a third party company to complete a task.
Overwriting	A method of sanitation and is used to replace previously stored data on the electronic media with a pattern of meaningless random or non-random information.
Personal Information	Recorded information about an individual **that renders that individual identifiable,** including: name, address, phone number; race, ethnic origin, or religious or political beliefs or associations; age, sex, sexual orientation, metal status, or family status; any identifying number or symbol; fingerprints, blood type, or inheritable characteristics; medial history; educational, financial, criminal, or employment history; personal views or opinions, except if they are about someone else; or anyone else's opinion about that individual.
Personal Information Bank	Any collection of personal information that is organized or retrievable by an individual's name, or by any identifying number, symbol, or other identifier assigned to an individual.
Personal Health Information Privacy and Protection Act (PHIPPA)	Ontario legislation created to install governance to support those in the health practice fields to protect the health information of patients which they acquire in the provision of health services.
Personal Information Protection and Electronic Documents Act(PIPEDA)	Federal legislation for the private sector meant to ensure personal information is collected and used in ways that secure and protect that information.
Policy	A high-level statement of intent.
Privacy	The quality or condition of being secluded from the presence or view of others. The state of being free from unsanctioned intrusion: a person's right to privacy.
Privacy Compliance Checklist	Provides considerations for assessing compliance in a structured format. By responding systematically to the specific questions or statements related to each privacy element, public bodies and trustees are able to review practices and determine what action may be needed to initiate or improve compliance.
Privacy Impact Assessment (PIA)	An assessment framework used to identify the actual or potential risks that a proposed or existing information system, technology, or program may have on an individual's privacy.
Privacy Standard	A set of rules, guidelines, and characteristics that helps to foster a culture of privacy regarding the way Ontario school boards/authorities collect, use, disclose, secure, retain, and dispose of personal information. It also ensures the right of individuals to have access to personal information about themselves and, as appropriate, to have it corrected.
Procedure	The approved steps required to accomplish the high-level statement of intent (policy).
Protocol	A code of correct conduct.
Purging	Cleaning out inactive or obsolete records or data from the set of active files (whether physical or computer based) for archiving or destruction (deletion). Also called culling.

Reception Equipment	Refers to the equipment or device used to receive or record the personal information collected through a video surveillance system, including a camera or video monitor or any other video, audio, physical, or other mechanical, electronic, or digital device.
Record	A document, regardless of physical format or characteristics, that memorializes and provides objective evidence of activities performed, events elapsed, results achieved, or statements made in the course of the organization's daily activities.
Record Classification	Process in which records are identified and categorized for filing on the basis of their subject matter and subject category, and are assigned a file number or code for efficient retrieval.
Records Management	Systematic administration of records and documented information for its entire life cycle, from creation/receipt, classification, use, filing, retention, storage, to final disposition. *See also: Document Management*
Records Control	The administration of documents, files, and records created or received by an organization in order to ensure proper authorization and procedure for having access to or handling of records.
Records Control Centre	A centralized location that is used for organized storage of inactive records retained for administrative or operating purposes, usually for a limited period of time. *See also: Remote Storage, Archives*
Records Disposition	*See: Disposition*
Records Inventory	List of all documents, files, and records created/received and maintained by an organization. It describes the title, function, purpose, content, date, format, and recording media, etc., and helps in the development of a record retention schedule.
Records Retention Period	The minimum amount of time to keep a record as determined to be necessary by law or other authority. Original records cannot be destroyed until the retention time has expired. Likewise, records should not be retained longer than the retention time without good reason.
Records Retention Schedule	A tool that describes (1) the length of time each document or record will be retained as an active record, (2) the reason (legal, fiscal, historical) for its retention, and (3) the final disposition (archival or destruction) of the record. Also called a record control schedule, record disposition schedule, or records schedule.
Records Transfer List	A form that tracks the whereabouts and disposition status of inactive records. This form constitutes evidence of authorized and regular disposition of records.
Remote Storage	Off-site storage of records in board-owned or commercial storage facilities. Applies to paper and electronic records.
Repository	Storage for indefinite or permanent placement. By comparison, a depository is storage in which something is placed to be taken out later.
Retrieval	The process of locating and accessing filed records.
Risk Management	The systematic application of management policies, procedures, and practices to the tasks of identifying, analyzing, assessing, treating, and monitoring risk.

Sanitizing	The removal of information from electronic media or equipment such that data recovery using standard techniques or analysis is prevented.
Sealed Records	Records protected by a court order which cannot be accessed or unsealed without another court order.
Scope Note	The component of a classification system that describes the function, uses, and content of records that are to be classified together.
Security Classification	Security level assigned to a government document, file, or record based on the sensitivity or secrecy of the information. Four common security classifications are: (1) Top secret: Highest degree of protection for information that is paramount in national defense matters and whose unauthorized disclosure may cause extremely grave danger or damage to the nation. (2) Secret: Unauthorized disclosure of which may result in serious damage or danger. (3) Confidential: Unauthorized disclosure of which may undermine defense or government operations.
Service Channel	Identifies the channel through which service/information is available (e.g., telephone, mail, in-person, Internet) and appropriate contact information for each channel.
Social Insurance Number (SIN)	A nine-digit number that one needs in order to work in Canada or to have access to government programs and benefits.
Standard	A set of rules, guidelines, and characteristics for activities or their results provided for common and repeated use. It is typically established by consensus and is usually a collective work created by bringing together the experience and expertise of all interested parties and stakeholders.
Structured Information	• IT perspective: Structured information refers to database-type information, where each field is defined and information entered into a field is always used in consistent ways by the application. • Reports, memos, letters, spreadsheets, etc., are structured by nature. The information within the document remains in a specific location at all times. • Structured information is most typically identified as databases, spreadsheets, and other formalized representations of information. Also included in this category may be forms (whether paper or electronic)-specifically, the information input into the form. Mail merge documents also fall into this category. *See also: Unstructured Information*
Sensitive Records	A record containing information considered private or confidential or which allows for identification of an individual. Examples include personnel files, student records, and litigation records. *See also: Personal Information Banks*
Storage Device	Refers to a video tape, computer disk or drive, CD-ROM, computer chip, or other device used to store the recorded data or visual, audio, or other images captured by a video surveillance system.
Superseded Record	A record is superseded when it is replaced with a new and up-to-date version (e.g., a procedure).

Technical Security Standard for Information Technology (TSSIT)	The RCMP TSSIT specifies security standards for information technology including media sanitization requirements. Media may be sanitized by using a software application that overwrites the media a minimum of three times by using a degausser or by physically destroying the media. *See also : Electromagnetic Degaussing, Sanitizing*
Third Party	A person or group who is not a party to a contract but who may become involved in an indirect way or be affected by it.
Third Party Personal	Refers to personal information about an individual that appears in conjunction with the personal information about one or more other individuals.
Third Party Service Provider	An external company or organization a school board/authority will "hire" to provide services, such as the warehousing of data.
Threat-Risk Assessment	An analysis that examines the different "threats" to an organization and identifies and corrects the most immediate and obvious security concerns.
Transitory Record	Routine correspondence and documents that have temporary usefulness and short term value and which are not incorporated into standard records control or filing systems.
Unified Messaging	A communication technology used for integrating voice mail into an organization's larger messaging environment (email) and computing infrastructure. This technology represents the convergence between voice and data communication systems in which email, voice mail, instant messaging, and other communications systems are integrated. The records/information management significance of this technology is that digitized voice mail messages require management as organizational records under retention and other organizational rules and policies.
Unstructured Information	• IT perspective: Unstructured information is more free-form and does not provide guidance as to how to find a certain type of information within the document. • Unstructured information includes most types of documents and records that do not fall into the category of structured information, including audio and video recordings, word processing documents, PowerPoint presentations, graphics, etc.
Video Surveillance System	A video, physical , or mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing, or monitoring of individuals in school buildings and on school premises (per IPC Video Surveillance Guidelines). Within the board, the surveillance system includes hand-held, portable digital devices used by principals and vice-principals to record school incidents for investigative purposes. Additional components of the surveillance system include portable video cameras that are used to record incidents on designated school buses from time to time as required.
Vital Records	A document, file, or record in any form or format, containing information that is (1) essential to the operations and/or survival of the organization, (2) necessary to recreate the organization's legal and financial position, and (3) necessary to preserve its claims and rights and those of its stakeholders. Also referred to as essential records.
Workflow	The documented flow of information in a business processes; the act of tracking work procedures through a fully documented process.

ACKNOWLEDGEMENTS

The Privacy and Information Management (PIM) taskforce would like to thank and acknowledge all participants who contributed their boundless time, creativity and focused commitment to the completion of the PIM toolkit. Without the commitment, dedication, hard work, and patience of all workgroup members, the PIM toolkit would not have been possible.

Privacy and Security Standards and Guidelines Workgroup

Rob Terhune	Sr. Analyst (A), IMB, Ministry of Education
Anthony Brice	Manager of Technology Systems, Kawartha Pine Ridge DSB
Rosanne Brown	Research Officer, Peel DSB
Sharron Christie	Manager, Admin, Thames Valley DSB
Sandra Connolly	MiSA Leader, PVNC DSB
Janice Currie	Sr. Manager, Professional Support Services, Toronto DSB
Kerry Haight	IT Integrator, Limestone DSB
Marianne Hendren	Senior Employee & Labour Relations Consultant, Kawartha Pine Ridge DSB
Cheryl Kennedy	FOI Manager, York Catholic DSB
Nancy Massie (Co-chair)	Records Manager, York DSB
Denis Menard	Coordonnateur, French MiSA
Colleen Norris	Co-ordinator of Policy Development, Windsor-Essex Catholic DSB
Laurie Schroeder	Manager, Admin., Waterloo Region DSB
Martine Pioffet	Adjointe Administrative, CSDCSO 58
Paul Podesta	MiSA Leader, Durham Catholic DSB
Sandra Quehl (Co-chair)	CIO, Waterloo Catholic DSB
Judy Selvadurai	Internal Auditor, York Catholic DSB

Privacy Impact Assessment Workgroup

Frances Boomhouwer	Trustee Liaison Officer/FOI & RM Administrator, Upper Canada DSB
Doug Brown	MiSA Leader, Waterloo Region DSB
Marie Clarke	MiSA Executive Lead, Thunder Bay Region MiSA PNC
Russ Coles (Co-chair)	Senior Manager of Computer Applications, York Region DSB

Shulin Dave	Manager - Project Services & MiSA Program Manager, Toronto DSB
Diane Findlay	Project Manager/Information Officer, Keewatin Patricia DSB
Steve Killip	Manager, Research, Assessment & Accountability, Thames Valley DSB
Lizanne Lacelle	Principal, Renfrew County DSB
Doris McWhorter	Research and Development Officer, Limestone DSB
Norma Townsend	Records Administrator, London District Catholic School Board
Rick Victor	Education Officer, Ministry of Education
Erica Van Roosmalen (Co-chair)	Chief Officer, Research & Development Service MiSA Lead, Halton Catholic DSB

Information Management Workgroup

Kellie Barron (Co-Chair)	ICT Director - Corporate Systems, Kawartha Pine Ridge DSB
Stephane Charbonneau	Coordonnateur GIARE, CSCNO 61
Gina Coish (Co-Chair)	FOI/RM Coordinator, Simcoe County DSB
Ralph Cuthbertson	Education Officer, Ministry of Education
Christine Downey	Manager ICT, Hamilton Wentworth Catholic DSB
Mark Hadwen	Information and Technology Services, Hastings and Prince Edward DSB
Shelley Hudson	MiSA Leader - Information and Innovation Services Supervisor, Greater Essex County DSB
Karen Huiberts	Human Resources Information Systems Analyst, London District Catholic School Board
Mike Kirby	Manager, Application Development & Support, Dufferin-Peel Catholic DSB
Etienne Lantos	MiSA Lead, Renfrew County DSB
Nancy Massie	Records Manager, York Region DSB
Kathleen O'Flaherty	Finance Manager, Keewatin-Patricia DSB
Nancy Sharpe	Manager of Communications, PVNC Catholic DSB
Andrea Stevenson	Manager of Information Services, Avon Maitland DSB
Tony Tuminieri	Education Officer, Ministry of Education
Claire Yancy	Secrétaire, École Mgr Augustin Caron et Membre de l'équipe GIARE, CSDECSO
Jeff Roynon	Data Analyst, Near North DSB

We would also like to thank Sharon Cohen, Shared Solutions Management Consulting, and Christine Ardern, Information Management specialists who gave generously of their time and expertise in consultation with the working groups.

Thank you to Jennifer Coens and Amy Coupal from Curriculum Services Canada. Curriculum Services Canada has been working tirelessly with us to bring it all together by publishing the toolkit and hosting our interactive website.

We owe a debt of gratitude to our legal counsel, Scott Williams (Hicks Morley) and Nadya Tymochenko (Keel Cottrelle), for their wise counsel, legal expertise and tremendous partnership at no cost to the taskforce. They have contributed an incredible number of hours to the toolkit and their knowledge and understanding of the business of school boards and culture has been instrumental in helping us to honour our guiding principles.

We also graciously thank the MiSA Professional Network Centres, CODE, OASBO and a number of individual school boards from across the province for funding the PIM initiative.

Finally, we would like to thank those who have actively championed the work of the PIM taskforce. Kathy Soule, Director of Hastings and Prince Edward District School Board, and Carol McAulay, Superintendent of Business, Simcoe County District School Board, agreed to be our champions and to bring briefings to CODE and COSBO on behalf of the taskforce.

Thank you from the PIM taskforce.

Gina Coish, Co-chair

Erica vanRoosmalen, Co-chair

Russ Coles, Finances

Kellie Barron

Nancy Massie

Denis Ménard

David Midwood

Sherri-Lynne Pharand

Sandra Quehl

Jeff Roynon

John Shanks