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")