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