

Date of Issue	February 2, 2010
Original Date of Issue	February 2, 2010
Subject	PRIVACY BREACH PROTOCOL
References	Policy 2197 – Management of Personal Information APM 1450 Management of Personal Information - Student
Links	FORM A1452-A; FORM A1450-2
Contact	Freedom of Information/Records Management Officer

Table of Contents

Item	Page
Item 1 Definitions	1
Item 2 Purpose	2
Item 3 Breaches.....	2
Item 4 Roles and Responsibilities in Responding to a Privacy Breach.....	3
Item 5 Response Protocol.....	4
FORM A1452 -1 Privacy Breach Report	9
FORM A1452 -2 Identity Theft Frequently Asked Questions	11

1. Definitions

1.1 **Privacy Breaches** occur when personal information is compromised, that is, when it is collected, used, disclosed, retained, or destroyed in a manner inconsistent with privacy legislation. Simply put, this means personal information has been accessed or viewed by someone who should not have access to it; or it has been collected without proper authority; or it has been used for purpose other than for which it was collected. Ontario school boards/authorities are governed by the following privacy statutes: *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and the *Personal Health Information Protection Act* (PHIPA).

1.2 **Personal information” (PI)** refers to information about an identifiable or potentially identifiable individual and includes, but is not limited to, personal health information and opinions about the individual.

1.3 **Personal health information** is information about an individual student that pertains to



health care, including information about a student's physical or mental health, receipt of health care services and health number.

1.4 **Third party service providers** include contracted third parties used to carry out or manage programs or services on behalf of the board and for the purposes of privacy breach reporting include all contractors that receive personal information from the board or collect personal information on behalf of the board, for example: school photographers; bus operators; external data warehouse services; or outsourced administrative services such as payroll or psychological services.

2. Purpose

This privacy breach protocol has been adopted to allow for a prompt, reasonable and coordinated response should personal information be breached. It will provide guidance on all reasonable steps necessary to limit the breach and is designed to clarify roles and responsibilities; support effective investigation and containment; and assist with remediation.

3. Breaches

Privacy breaches may be relatively obvious while others may not be as apparent. Examples of potential privacy breaches may include:

- 3.1 lost or misplaced personal information--for example, a misplaced student psychological assessment, report card or USB stick containing student marks, etc;
- 3.2 stolen technologies or equipment that may contain personal information--for example, laptops, data drives, disks, palms, etc;
- 3.3 disclosure of personal information to an unauthorized person or group--for example, student reports cards or verification sheets given to the wrong student(s), student marks emailed to wrong person, personal information posted publicly in error, etc;
- 3.4 deliberate disclosure of personal information to an unauthorized person or group for fraudulent or other purposes--for example, a user ID and password for access to personal information is posted on a social networking site, etc;
- 3.5 information used for a purpose not consistent with the reason the information was collected--for example, disclosure of staff contact list for purpose of sales and solicitation; or,
- 3.6 information collected in error—for example collected from a third party, or where there is no authorization for the collection.



4. Roles and Responsibilities

4.1 All Employees are responsible for:

- 4.1.1 being alert to the potential for personal information to be compromised, and playing a role in identifying, notifying, and containing a breach;
- 4.1.2 notifying their supervisor immediately, or, in his/her absence, the Freedom of Information Records Management Officer, upon becoming aware of a breach or suspected breach; and,
- 4.1.3 where possible, containing the suspected breach by suspending the process or activity that caused the breach to be determined on a case-by-case basis.

4.2 Principals and Managers are responsible for:

- 4.2.1 alerting the Superintendent and the FOI/Records Management Officer of a breach or suspected breach and working with the Officer to implement the five steps of the response protocol;
- 4.2.2 informing affected individuals if required, and responding to questions or concerns;
- 4.2.3 obtaining all available information about the nature of the breach or suspected breach, and determining what happened; and,
- 4.2.4 ensuring details of the breach and corrective actions are documented (see Form A1452-1).

4.3 The FOI/RM Officer is responsible for:

- 4.3.1 ensuring that all five steps of the response protocol are implemented;
- 4.3.2 supporting the Principal, Manager or Superintendent in responding to the breach;
- 4.3.3 notifying the Information and Privacy Commissioner where appropriate; and
- 4.3.4 responding to questions from the public regarding the breach.

4.4 Superintendent/Director or Designate is responsible for:

- 4.4.1 briefing senior management and trustees as necessary and appropriate;
- 4.4.2 reviewing internal investigation reports and approving required remedial action;
- 4.4.3 monitoring implementation of remedial action; and,
- 4.4.4 ensuring that those whose personal information has been compromised are informed as required.

4.5 Third Party Service Providers are responsible for:

- 4.5.1 taking reasonable steps to monitor and enforce their compliance with the privacy and security requirements defined in the contract or service agreement, and are required to inform their board contact of all actual and suspected privacy breaches;



- 4.5.2 informing their key contact and/or the FOI/RM Officer as soon as a privacy breach or suspected breach is discovered;
- 4.5.3 taking all necessary actions to contain the privacy breach as directed by the Director or designate;
- 4.5.4 documenting how the breach was discovered, what corrective actions were taken and reporting back;
- 4.5.5 undertaking a full assessment of the privacy breach in accordance with the third party service providers' contractual obligations;
- 4.5.6 taking all necessary remedial action to decrease the risk of future breaches; and,
- 4.5.7 fulfilling contractual obligations to comply with privacy legislation.

5. Response Protocol - Five Steps

These steps shall be initiated as soon as a privacy breach or suspected breach has been reported. Form A1452-1 shall be used to document the breach and guide the principal or manager through the breach management process.

5.1 Step 1 – REPORT AND ASSESS

5.1.1 Report

If you become aware of a possible breach of personal information by: 1) an internal source such as a staff member; or 2) an external source such as a third-party contractor, a parent or a student; the suspected breach shall be promptly reported to the principal or manager. This shall occur even if the breach is only suspected and not yet confirmed. The following information shall be included in the report:

- What happened?
- Where?
- When did the suspected incident occur?
- How was the potential breach discovered?
- Was any corrective action taken when the possible breach was discovered?

5.1.2 Assess

The Principal or Manager shall assess the breach by asking the following two questions. If the answer to **both** questions is yes, then it can be assumed that breach has occurred, the five-step protocol outlined in this procedure shall be followed and the Freedom of Information Records Management Officer shall be notified.

5.1.2.1 Is personal information involved?



Yes No

Not all board information is personal information. Refer to the definition of personal information in the definitions of this APM for assistance or consult with the FOI/RM Officer.

5.1.2.2 Has an unauthorized collection, use, disclosure or retention of personal information occurred?

Yes No

Unauthorized disclosure is the defining characteristic of a privacy breach. Regardless of whether it is intentional, accidental, or the result of theft or malicious intent, an unauthorized disclosure constitutes a privacy breach.

5.2 Step 2 – CONTAINMENT

5.2.1 Containment involves taking immediate corrective action to put an end to the unauthorized practice; for example: recovering the records; shutting down the system; revoking/changing computer access codes; or correcting weaknesses in physical or electronic security. The main goal is to alleviate any consequences for both the individual(s) whose personal information was involved and the Board.

5.2.2 All containment activities or attempts to contain shall be documented by the Principal or Manager on FORM A1452 - 1.

5.3 Step 3 – INVESTIGATE

Once the privacy breach is confirmed and contained the principal or manager shall conduct an investigation to determine the cause and extent of the breach by:

5.3.1 identifying and analyzing the events that led to the privacy breach;

5.3.2 evaluating if it was an isolated incident or if there is risk of further exposure of information;

5.3.3 determining who was affected by the breach; e.g. students or employees and how many were affected;

5.3.4 evaluating the effect of containment activities;

5.3.5 evaluating who had access to the information;

5.3.6 evaluating if information was lost or stolen; and,

5.3.7 evaluating if the personal information has been recovered.

5.4 Step 4 – NOTIFY

Notification helps to ensure that the affected parties can take remedial action if necessary and to support a relationship of trust and confidence. The Principal or Manager shall consult with the Superintendent and the Freedom of Information/Records Management Officer to determine what notifications are required. Considerations may include:

5.4.1 Notification to Authorities or Organizations

Examples of organizations that may need to be notified include: police if theft or other crime is suspected; insurers; Information and Privacy Commissioner; credit card companies and financial institutions; third party contractors or other parties that may be affected; other departments or staff; or, union or other employee groups.

5.4.2 Considerations for Determining if Notification is Required

In determining if notification to affected individuals is required, the following shall be considered:

5.4.2.1 Reasonable Expectations

The affected individual's reasonable expectation of notification shall be considered.

5.4.2.2 Who Had Access to the Breached Personal Information

Consideration shall be given to the recipient of the personal information for example individuals that are bound by professional duties of confidentiality or members of colleges that may be sanctioned if confidentiality is breached, i.e. a teacher who is a member of the College of Teachers; a psychologist who is a member of the College of Psychologists, etc.

5.4.2.3 Risk of Physical Harm

Does the loss or theft of information place any individual at risk of physical harm, stalking, or harassment?

5.4.2.4 Risk of Identity Theft

Is there a risk of identity theft or other fraud? 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, drivers' licence 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). (See FORM A1452-2).

5.4.2.5 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.

5.4.2.6 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?

5.4.3 Notification Timeline

Affected individuals shall be promptly notified. Depending on the nature and scope of the breach and status of the investigation, notification may occur in stages. For example, an initial notification may be given to ensure that the affected individuals receive information directly from the principal or manager with updates as required and a report of findings and action taken upon completion of the investigation.

5.4.4 Method of Notification

The method of notification shall be guided by the nature and scope of the breach and in a manner that reasonably ensures that the affected individual will receive it. Direct notification, e.g., by phone, letter, email or in person is preferable and shall be used where the individuals are identified. Where it is not possible to determine the affected individuals, for example when a student information system has been breached, posted notices, media releases, website notices or letters to all students or staff shall be considered.

5.4.5 Who is Responsible for Notification

Ideally the individual(s) shall be notified by the department associated with the breach. For example, where the breach is for student information, the Principal of the school shall be responsible for providing notification; where the breach is for staff information, Human Resource Services shall be responsible for providing notification. The Freedom of Information/Records Management Officer may be referred to as a contact for questions.

5.4.6 Notification shall include:

- 5.4.6.1 description of the incident and timing;
- 5.4.6.2 description of the information involved;
- 5.4.6.3 the nature of potential or actual risks or harm;
- 5.4.6.4 what mitigating actions were/are being taken;
- 5.4.6.5 appropriate action for individuals to take in order to protect themselves against harm;
- 5.4.6.6 a contact person for questions or to provide further information; and/or



5.4.6.7 contact information for the Information and Privacy Commissioner.

5.5 Step 5 – Prevention of Future Breaches

Once the breach has been resolved, the FOI/RM Officer shall work with the Principal, Manager or Superintendent to develop a prevention plan or take corrective actions if required. The extent of the response shall be determined by the significance of the breach and whether it was systemic or isolated. Responses may include: audits, review of policies, procedures and practices; employee training; or review of service delivery partners. Consideration shall be given to testing and evaluating remedial actions to determine if they have been implemented correctly and notifying the community of any changes or preventative measures that have been implemented.

Approved
Revised

January 2010

Issued under the authority of the Director of Education



PRIVACY BREACH REPORT

(to be completed by the Principal or Manager and forwarded to FOI/RM Officer)

Take immediate action when you have been advised of a suspected privacy breach.

Step 1. Report and Assess

Name of person reporting suspected breach (please print)

Job Title/Work Location

Supervisor

Person Incident Reported (if not to Supervisor)

Date and time incident discovered

Contact Number

What Happened?

Where?

When?

How was it discovered?

Action taken, if any.

Was personal information involved? yes no

Has an unauthorized breach occurred? yes no

If you answer yes to both questions, follow the protocol and complete the form. If not, no further action is required.

Step 2 Containment

Describe any actions taken to limit or contain the breach, for example "shut down the system", "retrieve copies of records", etc.

By whom?

Date

Time

Step 3 – Investigate

Who was affected, staff, students, contractors?

How many?

Describe the events lead to the breach and what form the breach took.

How was the information breached?



Step 4 – Notifications

Consult with the Freedom of Information/Records Management Officer or your Superintendent to confirm who should be notified and when.

Who should be notified (determined by the breach)?

- affected Individuals
- police if theft or other crime is suspected
- insurers or others
- information and Privacy Commissioner
- credit card companies, financial institutions
- third party contractors or other parties that may be affected
- other departments or staff
- union or employee bargaining groups

Notification to Affected Individuals shall include:

- description of the incident and timing
- description of the information involved
- nature of potential or actual risks or harm
- description of mitigating actions taken
- appropriate action for individuals to take to protect themselves against harm
- a contact person for questions or to provide further information
- contact information for the Information and Privacy Commissioner (if required)

Notification Provided by: _____

When: _____

How: _____

Step 5 – Prevention of Future Breaches

To be completed by the Principal or Manager.

Describe steps taken to prevent further problems.

Report completed by:

Principal or Manager (please print)

Superintendent

Date

Signature

Signature

FOI/RM Officer

Forward completed report to the FOI/RM Officer at the Education Centre

Identity Theft Frequently Asked Questions
For use when government issued ID or credit cards have been breached

What is Identity Theft?

Identity theft occurs when your personal information is used without your knowledge or consent to commit a crime such as fraud or theft. This may occur because identity thieves steal personal information and use it to impersonate you and commit crimes in your name. Identity thieves can manipulate your information and invade your personal and financial life. They can use stolen identity to conduct spending sprees, open a new bank account, divert mail, apply for loans, credit cards and social benefits, rent apartments and even commit more serious crimes.

In addition to names, addresses and phone numbers, identity thieves look for:

- Social insurance numbers;
- Driver's licence numbers;
- Credit card and banking information;
- Bank cards;
- Calling cards;
- Birth certificates;
- Passports.

What to do if Government Issued Documents are Lost or Stolen

If your birth certificate, driver's licence, social insurance card or any other government issued document is lost or stolen, notify the issuing authority right away so the document can be cancelled and a new one issued. You can also access this key contact information by visiting your nearest Ontario Government Information Centre or by phoning 414-326-1234 or toll-free 1-800-267-8097.

You may wish to take additional precautions such as placing a security/fraud alert on your credit bureau file, which flags the file for added security by potential lenders. You may also want to consider periodically obtaining a copy of your credit report and have any fraudulent transactions deleted. For your reference, the following is contact information for the three major credit card reporting agencies:

- Equifax – 1-800-525-6285
- Experian – 1-888-397-3742
- TransUnion – 1-800-680-7289

I've Taken All The Recommended Steps. Now What?

The following measures can help ensure that the identity theft is resolved and does not recur:

- Keep a log of all your phone calls. Write down the name of anyone you talked to, what he or she told you and the date your conversation occurred.
- In complex cases, you may want to follow up in writing with contacts you've made on the telephone or in person.
- Keep all originals of supporting documentation, like police reports and letters to and from companies. Send copies only.
- Keep old files even if you believe the case has been resolved. Errors can reappear on your credit reports or your information can be re-circulated.

Where Can I Get More Information About Identity Theft?

[Canadian Consumer Information Gateway](http://www.consumerinformation.ca/) - <http://www.consumerinformation.ca/>

[Safe Canada](http://www.safecanada.ca/identitytheft_e.asp) - http://www.safecanada.ca/identitytheft_e.asp

[Consumer Identity Theft Kit](http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00084.html) - <http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00084.html>