Date of issue	January 2024
Original date of issue	February 2010
Subject	**PRIVACY BREACH PROTOCOL**
References	Policy 2197 – Management of Personal Information APM A1450 – Management of Personal Information - Student
Contact	Business Services

1. 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.

2. Definitions

2.1 **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. Personal information has been accessed or viewed by someone who should not have access to it, collected without proper authority, or used for purposes 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).

2.2 **Personal information** - information about an identifiable or potentially identifiable individual and includes, but is not limited to, personal health information and opinions about the individual.

2.3 **Personal health information** - information about an individual that pertains to health care, including information about an individual's physical or mental health, receipt of health-care services, and health card number.

2.4 **Third-party service provider** - includes 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 (e.g., school photographers, bus operators, external data warehouse services, or outsourced administrative services such as payroll or psychological services).

3. Breaches

Some 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 (e.g., 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 (e.g., laptops, data drives, cellphones, etc.);

3.3 disclosure of personal information to an unauthorized person or group (e.g., student report 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 (e.g., 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 (e.g., disclosure of staff contact list for purpose of sales and solicitation); and,

3.6 information collected in error (e.g., 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 their absence, Business Services at privacy@scdsb.on.ca, 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 Business Services at privacy@scdsb.on.ca of a breach or suspected breach and working with Business Services 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 (FORM A1452 - 1).

4.3 Business Services is responsible for:
- 4.3.1 ensuring that all five steps of the response protocol are implemented;
- 4.3.2 supporting the principal, manager, and/or superintendent in responding to the breach;
- 4.3.3 notifying the Information and Privacy Commissioner where appropriate; and,
- 4.3.4 coordinating responses to questions from the public regarding the breach with the Communications department.

4.4 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 confirming 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;
- 4.5.2 informing their key contact and/or Business Services at privacy@scdsb.on.ca 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 an individual becomes aware of a possible breach of personal information by an internal source such as a staff member or an external source such as a third-party service provider, a parent/guardian, 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:

- 5.1.1.1 What happened?
- 5.1.1.2 Where?
- 5.1.1.3 When did the suspected incident occur?

5.1.1.4 How was the potential breach discovered?

5.1.1.5 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 a breach has occurred, the five-step protocol outlined in this procedure shall be followed, and the superintendent and Business Services at privacy@scdsb.on.ca 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 section 2 of this administrative procedures memorandum (APM) for assistance or consult with Business Services.

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 (e.g., 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 using 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 Business Services at privacy@scdsb.on.ca 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, the Information and Privacy Commissioner, credit card companies and financial institutions, third-party service providers or other parties that may be affected, other departments or staff, or union/ 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 (e.g., a teacher who is a member of the Ontario College of Teachers, a psychologist who is a member of the College of Psychologists of Ontario, 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, driver's license numbers, health card numbers, debit card numbers with password information, or any other information that can be used for fraud by third parties (e.g., financial).

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. Business Services 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,
- 5.4.6.7 contact information for the Information and Privacy Commissioner.

5.5 Step 5 – PREVENTION

Once the breach has been resolved, Business Services 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 third-party service providers. 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.

First issued January 2010
Revised October 2017, January 2024

Issued under the authority of the Director of Education

PRIVACY BREACH REPORT

(To be completed by the principal or manager and forwarded to Business Services at privacy@scdsb.on.ca)

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 to whom the incident was 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 the answer to both questions is yes, 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, (e.g., 'shut down the system', 'retrieve copies of records', etc.)

By whom? Date Time

Step 3 – Investigate

Who was affected (e.g., staff, students, service providers)?

How many?

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

How was the information breached?

Step 4 – Notifications

Consult with your superintendent or Business Services at privacy@scdsb.on.ca 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 service providers or other parties that may be affected
- ☐ other departments or staff
- ☐ union or other employee 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, manager, or superintendent.

Describe steps taken to prevent future breaches.

Report completed by:

Principal or manager (please print)	Signature
Superintendent	Signature
Date	Business Services

Forward completed report to Business Services at privacy@scdsb.on.ca