DDSB Ignite Learning

PROCEDURE

Governance (GOV)

PR GOV 06-02

Title: **Privacy Breach Procedure** *(Adopted under the Privacy Policy)*
Adopted: June 15, 2012
Effective: June 15, 2012
Amended/Reviewed: June 9, 2026

This procedure must be interpreted, applied, and implemented in ways that uphold Indigenous and human rights and responsibilities, promote accessibility, and prevent and address (and do not reinforce) discrimination/discriminatory barriers.

1.0 RATIONALE

This Privacy Breach Procedure has been adopted to allow for a prompt, reasonable and coordinated response should personal information be breached.

The Procedure is designed to:

a) provide guidance on all reasonable steps necessary to limit a breach;
b) clarify roles and responsibilities;
c) support effective investigation and containment; and,
d) assist with remediation.

This Procedure is to be interpreted and applied in accordance with the Durham District School Board's ("DDSB" or "the Board") commitment to promoting and upholding Indigenous rights and human rights in all of its learning and working environments. This includes anti-colonial, anti-discriminatory and anti-racist approaches and actions to provide services and employment that are safe, welcoming, respectful, inclusive, equitable, accessible and free from discrimination and harassment consistent with the DDSB's Human Rights, Anti-Discrimination and Anti-Racism Policy, the Indigenous Education Policy, and the Safe and Respectful Workplace and Harassment Prevention Policy.

2.0 DEFINITIONS

2.1 Personal Information (PI): recorded information about an identifiable individual and includes personal health information. As defined by the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), this may include, but is not limited to:

- Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, 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;
- Any identifying number, symbol or other particular assigned to the individual;
- The address, telephone number, fingerprints or blood type of the individual;
- The personal opinions or views of the individual except if they relate to another individual;
- 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;
- The views or opinions of another individual about the individual, and/or;
- The individual's name if it appears with other PI relating to the individual or where the Disclosure of the name would reveal other personal information about the individual.

2.2 Personal Health Information (PHI): has the meaning set out in s.4 of the Personal Health Information Protection Act (PHIPA). Specifically, it is "identifying information" about an individual that:

- Relates to the physical or mental health of the individual;
- Relates to the provision of health care to the individual;
- Is a plan of service under the Connecting Care Act, 2019, S.O. 2019, c. 5, Sched. 1;
- Relates to payments or eligibility for health care or eligibility for coverage for health care,
- Relates to the donation of any body part or bodily substance of the individual or that is derived from the testing or examination of any such body part or bodily substance;
- Is the individual's health number, and/or;
- Identifies an individual's substitute decision-maker.

PHI also includes identifying information about an individual that is not PHI listed above but that is contained in a record that includes PHI listed above. Information is "identifying" when it identifies an individual or when it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.

2.3 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: MFIPPA and the PHIPA.

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 purposes other than for which it was collected.

Some privacy breaches may be obvious while others may not be as apparent. Privacy breaches can involve personal information that the Board is holding, or personal information that a vendor is holding on behalf of the Board. Examples of potential privacy breaches may include:

2.3.1 lost or misplaced personal information – for example, a misplaced student psychological assessment, report card or USB stick containing student marks, etc.;

2.3.2 stolen technologies or equipment that may contain personal information – for example, laptops, data drives, disks, PDA's, etc.;

2.3.3 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.;

2.3.4 deliberate disclosure of personal information to an unauthorized person or group for fraudulent or other purposes – for example, theft of data (including theft of data held by one of the Board's vendors), a user ID and password for access to personal information is posted on a social networking site, etc.;

2.3.5 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 (including if personal information is used by one of the Board's vendors for a non-authorized purpose); or,

2.3.6 information collected in error – for example collected from a third party, or where there is no authorization for the collection.

2.4 Privacy Incident: a real or suspected privacy breach.

2.5 Service Provider: 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 collect, use or disclose personal information on behalf of the Board. For example: school photographers; bus operators; external data warehouse services; or extended daycare providers.

3.0 RESPONSIBILITY

3.1 All Employees

Responsible for:

3.1.1 being alert to the potential for PI to be compromised, and playing a role in identifying, notifying, and containing a breach;

3.1.2 notifying their supervisor immediately, or, in their absence, the Privacy Officer, upon becoming aware of a breach or suspected breach; and,

3.1.3 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.

3.2 Principals and Managers

Responsible for:

3.2.1 promptly alerting their Supervising Superintendent or Associate Director, Corporate Services as the case may be, and the Privacy Officer of a breach or suspected breach, and working with their Supervising Superintendent or supervisor to implement the five steps of the response protocol;

3.2.2 informing affected individuals if required, and responding to questions or concerns with input from the Supervising Superintendent and/or Privacy Officer as appropriate;

3.2.3 investigating with or without the assistance of the Privacy Officer and/or outside experts or providing outside investigators access to information;

3.2.4 for all incidents processed beyond Step 1 in the Response Protocol, completing and forwarding a Privacy Breach Report to the Privacy Officer; and

3.2.5 obtaining advice and guidance from the Privacy Officer as necessary to meet their responsibilities.

3.3 Supervising Superintendent/Associate Director

Responsible for:

3.3.1 ensuring that all five steps of the response protocol are implemented;

3.3.2 supporting the Principal or Manager in responding to the breach;

3.3.3 responding to questions from the public regarding the breach;

3.3.4 briefing senior management and trustees as necessary and appropriate;

3.3.5 reviewing internal investigation reports and approving required remedial action;

3.3.6 monitoring implementation of remedial action;

3.3.7 ensuring that those whose personal information has been compromised are informed as required; and

3.3.8 obtaining advice and guidance from the Privacy Officer as necessary to meet their responsibilities.

3.4 Privacy Officer

Responsible for:

3.4.1 providing legal advice and guidance to others with duties under this Procedure;

3.4.2 in consultation with the Associate Director, Corporate Services, retaining and instructing outside experts and investigators as appropriate;

3.4.3 as appropriate, and in consultation with the Associate Director of Corporate Services, reporting the breach to the Board's insurer;

3.4.4 reporting the Privacy Breach to the Information and Privacy Commissioner of Ontario where appropriate and coordinating with the applicable staff with respect to this reporting as appropriate;

3.4.5 working jointly with the Associate Director, Corporate Services, in liaising with service providers who are experiencing privacy incidents;

3.4.6 receiving and reviewing Privacy Breach Reports with a view to maintaining the Board's overall privacy protection program, and if litigation is contemplated, directing that the completion of a Privacy Breach Report be deferred, as appropriate; and

3.4.7 consulting with the Associate Directors on appropriate reporting to DDSB Chief Executive Officer and the Administrative Council on containment and mitigation issues in relation to any Privacy Breach.

4.0 APPLICATION AND SCOPE

This procedure applies to all DDSB employees and service providers who collect, use, disclose, retain, or manage personal information on behalf of the Board.

The procedure applies to actual and suspected privacy incidents involving personal information and personal health information governed by applicable privacy legislation, including incidents involving third-party service providers acting on behalf of the Board.

5.0 PROCEDURES

5.1 Response Protocol

The following five steps shall be initiated as soon as a Privacy Breach or Privacy Incident occurs:

1. Report and Assess
2. Containment
3. Investigate
4. Notify
5. Closure and Documentation

5.1.1 Step 1: Report and Assess

Report Breach

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 your Principal or Manager**. This shall occur even if the breach is only suspected and not yet confirmed. The following information shall be collected to include in the final documentation in Step 5:

a. What happened?
b. Where?
c. When did the Privacy Incident occur?
d. How was the Privacy Incident discovered?
e. Was any corrective action taken when the Privacy Incident was discovered?

Assess

The Principal or Manager shall assess the information collected to determine whether to take containment steps and notify the Privacy Officer.

If there is a possibility that PI has been collected, used or disclosed without authorization, the Principal or Manager shall take containments steps, per Step 2 below, and shall promptly notify the Supervising Superintendent and Privacy Officer.

5.1.2 Step 2 – Containment

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 the individual(s) whose PI was involved and for the Board.

5.1.3 Step 3 – Investigate

Once the privacy incident is contained, the Principal or Manager shall consider how best to investigate, with input from the Supervising Superintendent and/or the Privacy Officer as required.

If assistance from an outside expert or investigator is not required, the Principal or Manager shall gather evidence (documentation and statements) to determine the cause and potential impact of the breach by:

a. identifying and analyzing the events that led to the Privacy Breach;
b. evaluating if it was an isolated incident or if there is risk of further exposure to information;
c. determining who was affected by the breach, e.g. students or employees,

and how many individuals were affected;
d. evaluating the effect of containment activities;
e. evaluating who had access to what Personal Information;
f. evaluating if Personal Information was lost or stolen; and,
g. evaluating if the Personal Information has been recovered.

If the privacy incident involved personal information held by one of the Board's vendors, the Principal or Manager may need to seek all or some of the information above from the vendor.

5.1.4 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 Privacy Officer and the Supervising Superintendent (or the Superintendent of Education/Employee Relations for staff breaches, as appropriate) to determine what notifications are required.

Factors in assessing notification

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

a. Reasonable Expectation

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

b. Statutory Duties

If the information at issue is in a personal counselling or similar record the Board may have a statutory duty to notify affected individuals under the PHIPA. There is also notification duty in the Personal Health Information Protection and Electronic Documents Act that may be triggered in more rare circumstances.

c. Risk of Physical Harm

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

d. 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' 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). (Appendix 2).

e. 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.

f. *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?

Whether notification to authorities or organizations is required

The Privacy Officer shall notify the Information and Privacy Commissioner in accordance with any and all regulatory requirements. The Privacy Officer shall also provide notification to the following, as the Privacy Officer may deem appropriate depending on the circumstances:

a. police, if theft or other crime is suspected;
b. insurers;
c. credit card companies and financial institutions;
d. third party contractors or other parties that may be affected;
e. other DDSB departments or staff; or,
f. union or other employee groups.

Notification Timeline

Affected individuals shall be notified promptly after the Board determines that their PI has been collected, used, and disclosed without authorization.

Depending on the circumstances, notification may occur in stages. For example, the Board may choose to notify before completing an investigation if a suspected breach is widely known or if a breach is very likely. In doing so, the Principal or Manager should make clear what the Board knows and does not yet know, and commit to further follow-up.

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.

In certain cases, indirect notification may be appropriate. For example, the Board will consider indirect notifications where it is not reasonably possible to ascertain the entire population of affected individuals with precision, where there are a large number of individuals to notify, or where affected individuals are all impacted similarly. An indirect notification will be published prominently. The appropriate medium/media for an indirect notification will depend on the circumstances of the breach. Examples of public notices include posted notices, media releases, and website notices.

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 Supervising Superintendent or the Superintendent of Education / Employee Relations may be referred to as a contact for questions, as applicable.

Notification shall include:

a. description of the incident and timing;
b. description of the information involved;
c. the nature of potential or actual risks or harm;
d. what mitigation actions were/are being taken;
e. appropriate action for individuals to take in order to protect themselves against harm;
f. a contact person for questions or to provide further information; and/or,
g. contact information for the Information and Privacy Commissioner of Ontario.

5.1.5 Step 5 – Closure and Documentation: Prevention plan and corrective action

Once the breach has been resolved, the Supervising Superintendent or Associate Director, Corporate Services, as the case may be, shall work with the Principal or Manager to develop a prevention plan or take corrective actions, if required, and in doing so shall consult with the Privacy Officer.

The extent of the prevention plan or corrective actions shall be determined by the significance of the breach and whether it was systemic or isolated. These 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 a prevention plan or corrective actions to determine if they have been implemented correctly, as well as notifying appropriate stakeholders of any changes or preventative measures that have been implemented.

Privacy Breach Report

The Principal or Manager shall complete a Privacy Breach Report **(Appendix 1)** in consultation with the Privacy Officer and forward a final copy to the Privacy Officer. If litigation is contemplated, the Privacy Officer may direct that the completion of a Privacy Report be deferred.

Response Protocol – Service Providers

The Board will follow a similar process for responding to breaches and suspected breaches experienced by service providers. The response shall be led by the Privacy Officer delegate, who shall seek appropriate assurances from the service provider about:

a. The information the service provider will provide to the Board so it can meet its notification and other obligations to individuals;
b. The service provider’s plan for communication, which should not create

problems or challenges for the Board's own communication plan; and,

c. The final measures taken by the service provider to prevent a recurrence.

Litigation Considerations

These dealings with service providers may be taken in contemplation of litigation (and subject to litigation privilege).

6.0 APPENDICES

Appendix 1 – Privacy Breach Report Template

Appendix 2 – Identity Theft Frequently Asked Questions

7.0 REFERENCE DOCUMENTS

- DDSB P GOV 06 Privacy Policy
- DDSB PR GOV 06-01 Privacy Procedure (Personal)
- DDSB PR SCO 99-01 Acceptable and Safe Use Procedure for Computing Technology and Cyber Safety
- DDSB PR GOV 06-05 Network Access and Electronic Monitoring
- DDSB PR COM 01-02 Guidelines for E-Mail
- DDSB PR FIN 99-01 Staff Mobile Phones
- DDSB PR FAC 99-03 Video Surveillance System
- DDSB PR GOV 06-03 Technology Approval Process
- DDSB PR GOV 06-04 Technology Approval Process (Cloud Services): Privacy and Security Assessment Guide
- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- Personal Health Information Protection Act (PHIPA)
- Personal Information Protection and Electronic Documents Act (PIPEDA)