Privacy Protection and Information Access - Privacy Breach Procedures 315-C

Category: Administration
Administered by: Director of Education
First Adopted: June 2023
Revision History:
Next Review: 2027-28 School Year

1. General

Privacy is the right to control access to personal information and the right to decide what and how much information is shared with others, who it is shared with, and for what purposes.

The *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) set out rules that persons or organizations must follow when collecting, using, disclosing, retaining, and disposing of personal information and/or personal health information. These Acts balance the rights of individuals to their privacy, with the legitimate needs of staff in organizations to collect, use and share information to conduct their work. These Acts also require organizations to take reasonable steps to ensure that information in their custody or control is protected against theft, loss, unauthorized use or disclosure, modification, or disposal.

The types of privacy breaches that may occur and the procedure to follow when there has been a breach at the UGDSB is outlined below.

2. Definitions

Privacy Breach
A privacy breach occurs when personal information is collected, used, disclosed, retained or destroyed in a manner inconsistent with privacy legislation.

Personal Information
Personal information means recorded information about an identifiable individual including:

- information relating to their 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 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

Privacy Protection and Information Access Handbook
The Privacy Protection and Information Access Handbook for UGDSB staff outlines the procedures to be undertaken by all employees in order to protect all personal information in the board's custody and control from unauthorized access, disclosure and inadvertent destruction. As one resource available for staff training, this handbook contains information from a number of the board's policies and procedures relating to confidentiality, privacy and information access, as well as physical and technical security. It also contains a description of the current legislative framework governing personal information in Ontario, including personal health information, and a summary of the ten (10) privacy commitments that shape current information privacy practices at the board.

Record
A record refers to any documented information in any format, including print, film or electronic, that is in the custody and/or control of the organization (e.g., email correspondence, memos, plans, maps, drawings, diagrams, pictures, graphic work, photographs, videos, microfilm, sound recording, machine readable records, and any other documentary material).

3. Privacy Breaches

Personal information can be compromised in many ways. Some privacy breaches have relatively simple causes and are contained, while others are more systemic or complex. Privacy breaches are often the result of human error.

3.1 Examples of privacy breaches may include, but are not limited to:

- electronic device (i.e., laptop, cell phone, tablet or iPad) left in a public area containing student data or other personal or confidential information
- electronic device containing personal information is stolen
- documents containing personal information left unattended on a photocopier
- reports containing personal information are found in recycle or garbage bins
- confidential documents left in public view on an employee's desk or other publicly accessible area
- report card or confidential letter addressed to person A is mailed or given to person B
- records destroyed prior to their required retention
- students' personal information shared with a third party (e.g., vendor or web application) without notice or informed consent of a parent or guardian or adult student.

3.2 If an individual whose personal information, or whose child's personal information, was breached, believes that the board has failed to comply with one or more of the privacy protection provisions of privacy legislation, and that their (or their child's) privacy has been compromised as a result, the individual can file a complaint with the Information and Privacy Commissioner of Ontario (IPC). As well, upon learning of a possible privacy breach, the IPC may itself initiate an investigation in the absence of an individual complaint.

4. Privacy Breach Response Procedure

When a staff member suspects that a privacy breach has occurred, they have a responsibility to notify their supervisor immediately, or in their absence, contact the board's Freedom of Information (FOI) Coordinator at (519) 822-4420. Contain, if possible, the suspected breach by delaying or suspending the process or activity involving the exposure or mishandling of student or employee personal information. Senior administration, managers and principals are to alert the FOI Coordinator of a suspected breach; obtain all available information about the nature of the suspected breach; follow the board's privacy breach procedure, complete a Privacy Breach Report and work with the FOI Coordinator to implement the five steps listed below.

4.1 Step 1 – Respond

4.1.1 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, immediately contact the appropriate supervisory staff and the FOI Coordinator for further instruction.

4.2 Step 2 – Contain

4.2.1 Identify the scope of the breach and if possible, contain it (e.g., remove personal information from a website).

4.2.2 Document the breach and containment activities; develop briefing materials.

4.2.3 Retrieve the information if the records are in hard copy.

4.2.4 Ensure that no copies were made by whomever had access to the information

4.2.5 Obtain contact information of the unauthorized person/party in case follow-up is needed.

4.2.6 Brief the accountable decision maker (director or superintendent), and key persons on the privacy breach and how it is being managed.

4.2.7 Determine if the breach would allow unauthorized access to any other personal information. It may be necessary to temporarily shut

down a system or remove access to the server until the breach is contained.

4.3 Step 3 – Investigate

4.3.1 Once the privacy breach is contained, conduct an investigation with the involvement of other board departments/staff, or legal counsel, as necessary (i.e., whose information was involved, how many people).

4.3.2 Identify and analyze the events that led to the privacy breach and evaluate the risk of exposure.

4.3.3 Note if it was a systemic breach (e.g., network security failure), or an isolated incident (e.g., lost folder).

4.3.4 Determine what types of data were involved and how sensitive it is (e.g., age and gender vs. medical information).

4.3.5 Determine if the data could be used for fraudulent or otherwise harmful purposes (e.g., identity theft, access to systems/devices, public humiliation).

4.3.6 Evaluate what was done to contain the breach and recommend remedial action so future breaches do not occur.

4.3.7 Complete the Privacy Breach Report, as outlined in the Privacy Protection and Information Access Handbook, for record keeping.

4.4 Step 4 – Notify

4.4.1 Notify, as required, the individuals whose personal information was disclosed using the best method (e.g., telephone or in writing). Providing notice of a privacy breach to the individual(s) whose personal information was involved in the incident should include an apology for the breach while personal information was in the board's custody, and information about:

- what happened, including details regarding the extent of the breach and type of data
- the nature of potential or actual risks or harm

- what mitigating actions the board is taking; and
- appropriate action for individuals to take to protect themselves against harm

4.4.2 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. Explain the individual's right to complain to the IPC about the board's handling of their personal information, along with contact information for the IPC.

4.4.3 Notify appropriate managers and employees within the board of the breach.

4.4.4 Report the privacy breach to the office of the IPC as appropriate (refer to the Privacy Protection and Information Access Handbook to determine if notification is required).

4.5 Step 5 – Implement Change

Determine what changes and remedial actions need to be implemented. It may be necessary to:

4.5.1 Review the circumstances surrounding the breach. Ensure the immediate requirements of containment and notification have been addressed.

4.5.2 Review the relevant information management systems to enhance compliance with privacy legislation.

4.5.3 Amend or reinforce the existing policies, procedures, and practices for managing and safeguarding personal information.

4.5.4 Develop and implement new security or privacy measures, if required.

4.5.5 Review employee training on legislative requirements, security and privacy policies, procedures, and practices to reduce potential of future breaches, and strengthen as required.

4.5.6 Test and evaluate remedial actions to determine if they have been implemented correctly and if policies, procedures, and practices need to be modified.

4.5.7 Recommend remedial action to the accountable decision maker.

5. Staff Responsibilities

5.1 All Staff

5.1.1 All UGDSB staff need to be alert to the potential for personal information to be out-of-place. Employees play a vital role in identifying, notifying, containing, and remediating a breach.

5.1.2 In case of a breach or suspected breach, employees must notify their supervisor and/or the Privacy Officer immediately.

5.1.3 Work with supervisor and Privacy Officer to implement breach response protocol.

5.2 Superintendents, Managers, and Principals

5.2.1 Alert the Director of Education and/or Privacy Officer of a breach or suspected breach.

5.2.2 Work with staff and Privacy Officer to implement the breach response procedure outlined in section 4.

5.3 Director of Education

5.3.1 Brief senior management and trustees as necessary and appropriate.

5.3.2 Review internal investigation reports and approve required remedial action.

5.3.3 Monitor implementation of remedial action and ensure that all five steps of the breach response protocol are followed.

5.4 Privacy Officer

5.4.1 Work with affected staff to implement the breach response procedure.

5.4.2 Ensure that all five steps of the breach response procedure are implemented and make recommendations for remediation.

5.4.3 Provide a report to senior administration on the progress and outcome of the breach response and where appropriate, report the breach to the office of the Information and Privacy Commissioner of Ontario.

5.4.4 Track privacy breaches and details of breach responses.

5.4.5 Determine when notifications are applicable and ensure they are carried out.

5.4.6 Promote changes in practice that reduce breach risk and monitor the implementation of changes.

5.4.7 Maintain the Privacy Protection and Information Access Handbook for staff.