Lambton Kent District School Board

ADMINISTRATIVE PROCEDURES

SUBJECT: PRIVACY BREACH PROTOCOL

PREAMBLE

The Lambton Kent District School Board is committed to ensuring the protection of personal information in its custody and control.

The following procedures outline the necessary steps to contain and respond to incidents involving the unauthorized disclosure of personal information. Employees have a role and responsibility to assist in the containment of a privacy breach.

DEFINITION

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 or can involve technology/ computer error. The following are some examples of privacy breaches: student report card mailed to the wrong home; hard copy psychological assessments kept in openly accessible file cabinets that are not secured or controlled; theft from a car of a briefcase containing a list of home addresses of teaching staff; lost memory key containing student data; or theft from a teacher's car of a laptop containing Special Education student records.

ROLES AND RESPONSIBILITIES

Employees

All employees need to be alert to the potential of personal information being compromised, and therefore potentially play a role in identifying, notifying and containing a breach. Employees must notify their supervisor immediately, or, in his/her absence, the Board's FOI Coordinator upon becoming aware of a breach or suspected breach.

Employees dealing with student, employee and/or business records need to be particularly aware of how to identify and address a privacy 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.

The FOI Coordinator will follow the following five steps: Respond, Contain, Investigate, Notify and Implement Change.

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 Board's roles, responsibilities and the response plan. The Director of Education is the accountable decision maker.

Third Party Service Providers

In many instances the Board uses contracted third party service providers to carry out or manage programs or services on its 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, the Board retains 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 the Board of all actual and suspected privacy breaches.

The third party service providers have the responsibility to:

- inform the Board 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 Board.
- 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.

The FOI Coordinator will work with appropriate staff to implement concurrently the five steps of the Response Protocol

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 Board (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 Board'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 the individual(s) as soon as possible if personal health information is stolen, lost, used or disclosed without authority. Include in the notice a statement that the individual is entitled to make a complaint to the Ontario Privacy Commissioner.
- Notify, as required, the individuals whose personal information (non-health) was disclosed if it is determined that 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 Board's handling of their personal information, along with contact information for the IPC.

- Notify appropriate managers and employees within the Board of the breach;
- Report the privacy breach to the office of the Information and Privacy Commissioner (IPC) as appropriate.
- Breaches involving the theft, loss or unauthorized use or disclosure of personal health information must be reported to the Privacy Commissioner (IPC) if there are reasonable grounds to believe that: there was intentional misuse of information; theft of information; containment issues where the personal health information was or could be further used or disclosed without authority; systemic problems where there is a pattern of similar losses or unauthorized use or disclosure; or if the breach is deemed to be significant (sensitivity/volume).

- Notify governing college of a Health Information Custodian (HIC)/agent who is a member of a college if the employee is terminated, suspended or subject to disciplinary action as a result of the unauthorized collection, use or disclosure of personal health information; or if the employee resigns and it is believed that the resignation is related to investigation of a breach involving personal health information.

The following factors should be considered by the FOI Coordinator when determining whether notification is required:

- **Personal Health Information**

  Does the breach involve the theft, loss or unauthorized use or disclosure of personal health information?

- **Risk of Identity Theft**

  Is there a risk of identity theft or other fraud in the Board? 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?

Step 5 – Implement Change

When determining what changes and remedial actions need to be implemented, the FOI Coordinator in consultation with the Board's PIM Champion will 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.

Implementation Date: April 6, 2010
Revised: March 2018

Reference: Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
Personal Health Information Protection Act (PHIPA)
Personal Information Protection and Electronic Documents Act (PIPEDA)