PROCEDURE SO105

Privacy Breach Response

Board Received: June 22, 2020 **Review Date:** September 2024

Accountability

1. Frequency of Reports – As needed.
2. Criteria for Success – Staff members understand the process to follow when privacy breaches occur.

1.0 Purpose

The Grand Erie District School Board is committed to the protection of personal information under its control and to the individuals' right of privacy regarding personal information that is collected, used, disclosed and retained in the school system.

The *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* and the *Personal Health Information Protection Act (PHIPA)* set out rules that persons and/or organizations must follow when collecting, using, disclosing, retaining and disposing of personal information.

This privacy breach procedure has been adopted to allow for a prompt, reasonable and coordinated response should personal information be breached. It is designed to clarify roles and responsibilities, and support effective containment, investigative, and remediation activities.

2.0 Definition of a Privacy Breach

A privacy breach occurs when personal information is compromised; when it is collected, accessed, used, disclosed, lost, retained or destroyed in a manner inconsistent with privacy legislations.

Personal information can be compromised in many ways. Some breaches are relatively simple in cause and are contained, while others are more systemic or complex. Privacy breaches are often the result of human error, such as an individual's personal information sent by mistake to another individual. A breach can be more wide scale, such as when an inappropriately executed computer programming change causes personal information of many individuals to be compromised through inadvertent distribution.

3.0 Roles and Responsibilities in Responding to Privacy Breaches

Individuals	Roles	Responsibilities
3.1 **Employees**	Employees dealing with student, employee and/or business records need to be particularly aware of how to identify and address a privacy breach. Employees must comply with the board's approval process for use of online education services to avoid	All Grand Erie employees are responsible to: • notify their supervisor immediately, or, in their absence, the Freedom of Information (FOI) Coordinator upon becoming aware of a breach or suspected breach; and

	exposing the board to reputational/digital privacy risks	• contain, if possible, the suspected breach by suspending the process or activity that caused the breach.
3.2 **Superintendents, Principals, and Managers**	Superintendents, Principals, and Managers have the ultimate responsibility to alert the FOI Coordinator of a breach or suspected breach and to work with the FOI Coordinator to implement the five steps of the Privacy Breach Protocol	Superintendents, Principals, and Managers have the responsibility to: o obtain all available information about the nature of the breach or suspected breach and determine what happened; o alert the FOI Coordinator and provide as much information about the breach as is currently available; o work with the FOI Coordinator to undertake all the appropriate actions to contain the breach; and o ensure details of the breach and corrective actions are documented.
3.3 **FOI Coordinator**	FOI Coordinator plays a central role in the response to a breach by ensuring that all five steps of the response procedure are implemented (see Response Procedure)	The FOI Coordinator will follow the following five steps: Step 1 – Respond Step 2 – Contain Step 3 – Investigate Step 4 – Notify Step 5 – Implement Change
3.4 **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. For Grand Erie, the Director of Education is the accountable decision maker	The Director of Education has the responsibility to: o brief senior management and trustees, as necessary and appropriate; o review internal investigation reports and approve required remedial action; o monitor implementation of remedial action; and o ensure that those whose personal information has been compromised are informed as required.
3.5 **Third Party Service Providers**	Examples of third-party service providers include: o educational technology applications; o commercial school photographers; o bus companies; o external data warehouse services; o outsourced administrative services (such as cheque production, records storage, shredding services; o Children's Aid Society (CAS);	The third-party provider, in conjunction with the board, has the responsibility to: o inform the board as soon as a privacy breach or suspected breach is discovered; o take all necessary actions to contain the privacy breach as directed by the board; o document how the breach was discovered, what corrective actions were taken and report back to their Board point of

	○ Settlement Workers; ○ Public Health Units (PHU); ○ External researchers & consultants. Grand Erie has the responsibility to ensure all third-party service providers are in compliance with privacy obligations, including an agreed-upon breach protocol between the two parties. Third party service providers must be aware of their roles and responsibilities if a privacy breach occurs when they have custody of personal information. Third party service providers must monitor and enforce compliance with the privacy and security requirements defined in contracts or service agreements and are required to inform Grand Erie of all actual and suspected privacy breaches.	contact or the Board's FOI Coordinator; ○ undertake full assessment of the privacy breach in accordance with third party service provider's contractual obligations ○ take all necessary remedial action to decrease the risk of future breaches; and ○ fulfill contractual obligations to comply with privacy legislation.

4.0 Privacy Breach Response Protocol

The following five actions are to be initiated as soon as a privacy breach or suspected breach has been reported to the FOI Coordinator. The FOI Coordinator will:

4.1 Step 1: Respond/Assess

- Work with the school/department to assess the situation to determine if a breach has indeed occurred;
- Provide advice on what steps to take to respond to the breach; and
- Report the privacy breach to key persons within the Board and, if necessary, law enforcement.

4.2 Step 2: Containment

- Identify the scope of the breach and take corrective steps to contain it.
- Activities may include:
  - Recovering records
  - Revoking/changing computer access codes
  - Correcting weaknesses in physical or electronic security
- All containment activities or attempts to contain shall be documented by the Principal, Manager or any other individual(s) involved in containing the breach and report back to the FOI Coordinator

4.3 Step 3: Investigate

Once the privacy breach is contained,

- Identify the events that led to the privacy breach;
- Evaluate the risk of the exposure;
- Determine if the breach was benign (e.g. human error, accidental) or malicious (e.g. deliberate sabotage, hacking);

- Determine who was affected by the breach (e.g. students or employees) and how many were affected, what types of data were involved and how sensitive it is (e.g. age, gender vs. medical information);
- Identify who had access to the information; and
- Evaluate the effect of containment activities.

4.4 Step 4: Notify

Notification helps to ensure affected parties can take remedial action, if necessary, and to support a relationship of trust and confidence. Notification will involve the following considerations:

- Principal and Manager will consult with the FOI Coordinator to determine what notifications are required;
- Affected individuals shall be notified promptly and, depending on the nature/scope of the breach, notification may occur in stages;
- 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 (i.e.: by phone, letter, email or in person);
- Individual(s) shall be notified by the department associated with the breach (i.e.: student information by the Principal, employee information by Human Resources);
- Notification shall include:
    - Description of the incident and the personal information involved
    - Nature of potential or actual risk or harm, if any, and the appropriate action for individual(s) to take to protect themselves
    - What steps/actions were/are being taken
    - A contact person for questions or to provide further information; and/or contact information for the Information and Privacy Commissioner, as appropriate

4.5 Step 5: Implement Change

- Review the circumstances surrounding the breach. Ensure the immediate requirements of containment and notification have been addressed;
- Develop and implement new security or privacy measures;
- Determine if any systemic practices or procedures warrant reviews;
- Test and evaluate remedial actions to determine if implemented correctly; and
- Ensure staff are properly trained in new safeguards.

Resources:

- *Information and Privacy Commissioner/Ontario, Breach Notification Assessment Tool, December 2006*
- *Information and Privacy Commission/Ontario, What to do if a Privacy Breach Occurs: Guidelines for Government Organizations, May 2003*