PROCEDURE IT-003

PRIVACY BREACH RESPONSE	
Superintendent Responsible: Superintendent of Education, Privacy and Information Management	**Initial Effective Date:** 2020/06/22
Last Updated: 2023/06/29	**Next Review Date:** 2027/06/25

Purpose:
The Grand Erie District School Board (Grand Erie) 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.

Guiding Principles:
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 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.

1.0 **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 means recorded information about an identifiable individual, including, but not limited to:

1.1 Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual.

1.2 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.

1.3 Any identifying number, symbol or other particular assigned to the individual.

1.4 The address or telephone number of the individual.

1.5 The personal opinions or views of the individual except if they relate to another individual.

1.6 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.

1.7 The views or opinions of another individual about the individual.

1.8 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.

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.

2.0 **Roles and Responsibilities in Responding to Privacy Breaches**

Individuals	Roles	Responsibilities
Employee(s)	Employee(s) dealing with student(s), employee(s) and/or business records need to be particularly aware of how to identify and address a privacy breach. Employees must comply with the Grand Erie's approval process for use of online education services to avoid exposing the board to reputational/digital privacy risks.	All Grand Erie employee(s) are responsible to: • notify their Supervisor(s) immediately, or, in their absence, the Manager of Privacy and Director Services upon becoming aware of a breach or suspected breach; and • contain, if possible, the suspected breach by suspending the process or activity that caused the breach.
Superintendent(s), Administrator(s), and Manager(s)	Superintendent(s), Administrator(s), and Manager(s) have the ultimate responsibility to alert the Manager of Privacy and Director Services of a breach or suspected breach and to work with the Manager of Privacy and Director Services to implement the five steps of the Privacy Breach Protocol.	Superintendent(s), Administrator(s), and Manager(s) have the responsibility to: • obtain all available information about the nature of the breach or suspected breach and determine what happened • alert the Manager of Privacy and Director Services and provide as much information about the breach as is currently available • work with the Manager of Privacy and Director Services to undertake all the appropriate actions to contain the breach; and • ensure details of the breach and corrective actions are documented.
Manager of Privacy and Director Services	The Manager of Privacy and Director Services plays a central role in the response to a breach by ensuring that all five steps of the response procedure are implemented	The Manager of Privacy and Director Services will follow the following five steps: Step 1 – Respond Step 2 – Contain Step 3 – Investigate Step 4 – Notify Step 5 – Implement Change
Accountable Decision Maker	The responsibility for protecting personal information affected by a privacy breach is assigned to the Manager of Privacy and Director Services. This individual is the key decision maker in responding to privacy breaches.	The Manger of Privacy and Director Services has the responsibility to: • brief the Senior team who, as necessary and appropriate • review internal investigation reports and approve required remedial action • monitor implementation of remedial action • ensure that those whose personal information has

		been compromised are informed as required
Third-Party Service Providers	Examples of third-party service providers include: • educational technology applications • commercial school photographers • bus companies • external data warehouse services • outsourced administrative services (such as cheque production, records storage, shredding services • Children's Aid Society (CAS) • Settlement Workers • Public Health Units (PHU) • External researchers and 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.	The third-party provider, in conjunction with Grand Erie has the responsibility to: • inform Grand Erie as soon as a privacy breach or suspected breach is discovered • take all necessary actions to contain the privacy breach as directed by Grand Erie • document how the breach was discovered, what corrective actions were taken and report back to their point of contact or the Manager of Privacy and Director Services • 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

3.0 **Privacy Breach Response Protocol**

The following five (5) actions are to be initiated as soon as a privacy breach or suspected breach has been reported to the Manager of Privacy and Director Services. The Manager of Privacy and Director Services will:

3.1 **Step 1: Respond/Assess**

3.1.1. Work with the school/department to assess the situation to determine if a breach has indeed occurred.

3.1.2. Provide advice on what steps to take to respond to the breach.

3.1.3. Report the privacy breach to key persons within Grand Erie and, if necessary, law enforcement.

3.2 **Step 2: Containment**

3.2.1. Identify the scope of the breach and take corrective steps to contain it.

3.2.2. Activities may include:

- recovering records
- revoking/changing computer access codes
- correcting weaknesses in physical or electronic security

3.2.3. All containment activities or attempts to contain shall be documented by the Administrator(s), Manager or any other individual(s) involved in containing the breach and report back to the Manager of Privacy and Director Services.

3.3 **Step 3: Investigate**

Once the privacy breach is contained:

3.3.1. Identify the events that led to the privacy breach.

3.3.2. Evaluate the risk of exposure.

3.3.3. Determine if the breach was benign (e.g., human error, accidental) or malicious (e.g., deliberate sabotage, hacking).

3.3.4. 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).

3.3.5. Identify who has access to the information.

3.3.6. Evaluate the effect of containment activities.

3.4 **Step 4: Notify**

3.4.1. 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:

- Administrator(s) and Manager will consult with the Manager of Privacy and Director Services 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 Administrator(s), 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

3.5 **Step 5: Implement Change**

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

3.5.2. Develop and implement new security or privacy measures.

3.5.3. Determine if any systemic practices or procedures warrant reviews.

3.5.4. Test and evaluate remedial actions to determine if implemented correctly.

3.5.5. Ensure employees are properly trained in new safeguards.

3.6 **Step 6: Complete Privacy Breach Reporting Form**

3.6.1. Once Step 1 – 5 have been completed and consultation with the Manager of Privacy and Director Services has occurred, complete the **online form** by entering as much detail about the incident as possible including any follow-up actions taken.

Reference(s):

- Acceptable Use of Information Technology Policy (IT-01)
- Acceptable Use of Information Technology Procedure (IT-001)
- Information and Privacy Commissioner of Ontario, Breach Notification Assessment Tool, December 2006
- Information and Privacy Commission of Ontario, What to do if a Privacy Breach Occurs: Guidelines for Government Organizations, May 2003
- *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56*
- Privacy and Records Information Management Policy (IT-02)