Peterborough Victoria
Northumberland and Clarington
Catholic District School Board

BOARD ADMINISTRATIVE PROCEDURE	
Administrative Procedure **Privacy Breach Response**	Administrative Procedure Number **1209**
Directional Policy **Records and Information – 1200**	

TITLE OF ADMINISTRATIVE PROCEDURE:

Privacy Breach Response

DATE APPROVED:

May 26, 2020

PROJECTED REVIEW DATE:

May 2025

DIRECTIONAL POLICY ALIGNMENT:

The Privacy Breach Response Administrative Procedure supports Directional Policy 1200 - Records and Information by supporting protection of privacy and the Board's efforts to strategically maintain records and information, adhere to relevant privacy legislation and ensure the efficient creation, maintenance, retrieval, security, storage, and disposition of records.

ALIGNMENT WITH MULTI-YEAR STRATEGIC PLAN:

The Privacy Breach Response Administrative Procedure supports our Vision for achieving Excellence in Catholic Education by supporting the Board's commitment to maintaining a reliable and accessible record of Board actions, transactions and

decisions through a coordinated and integrated approach to records and information management.

Strategic Priorities 2017-2020

Vision

Achieving Excellence in Catholic Education
LEARN • LEAD • SERVE

Mission

To educate students in faith-filled, safe, inclusive Catholic learning communities by nurturing the mind, body and spirit of all.

LEARN

Achieve excellence in instruction and assessment to enable all students to become reflective, self-directed, lifelong learners.

LEAD

Foster critical thinking, creativity, collaboration, and communication, to enable all students to realize their God-given potential.

SERVE

Inspire engagement and commitment to stewardship for creation to enable all students to become caring and responsible citizens.

ACTION REQUIRED:

Peterborough Victoria Northumberland and Clarington (PVNC) Catholic District School Board is committed to the protection of personal and confidential information under its custody or control and to an individual's right of privacy regarding personal information that is collected, used, retained and disclosed in the school system.

While protection of personal information is paramount, the board recognizes that breaches will occur. This Privacy Breach Response Administrative Procedure allows for a prompt, reasonable and coordinated response when personal information is compromised; that is, when it is collected, accessed, used, disclosed, retained, or destroyed in a manner inconsistent with privacy legislation.

All employees, members of the Board and third-party providers have a role and responsibility to assist in the containment of a privacy breach.

This administrative procedure outlines the action to be undertaken immediately should a privacy breach or suspected breach occur. It describes the steps necessary to limit the breach and is designed to clarify roles and responsibilities, support effective investigation and containment, and assist with remediation.

PRIVACY BREACH:

a. A privacy breach occurs when personal information is collected, used, disclosed, retained, or destroyed in a manner inconsistent with privacy legislation. PVNC is governed by the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and Personal Health Information Protection Act (PHIPA). These acts govern the collection, use, disclosure and security of personal information.

b. 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, such as an individual's personal information being sent by mistake to another individual. In today's environment in which technology increasingly facilitates information exchange, a privacy breach can be more wide-scale.

Examples of potential privacy breaches include:

i. Lost or misplaced personal information, such as a misplaced student assessment, report card or Ontario Student Record (OSR) or a lost USB stick containing student marks or employee contact information.
ii. Stolen technologies or equipment such as laptops, iPads or smart phones that may contain personal information.
iii. Disclosure of personal information to an unauthorized person or group, such as student information forms given to the wrong students or personal information disclosed to a board member, employee or outside agency who did not need it to effectively decide on a matter.
iv. Inappropriate disclosure of personal information, such as two employees discussing and identifying a student in a grocery store, or similar conversation on a cell phone in a public place.
v. Information used for the purpose not consistent with the reason it was collected, such as sharing of staff or contact information for the purpose of sales or marketing or providing personal student information for a third party sponsored contest, without informed consent.

vi. Disposal of equipment with memory capabilities, such as USB sticks, laptops or photocopiers, or paper records containing personal information in a non-secure manner.
vii. Disclosure of personal information via any electronic, message-based or social threat such as ransomware, phishing or extortion.

RESPONSIBILITIES:

All employees and members of the Board are responsible for:

- Being alert to the potential for personal information to be compromised, and therefore potentially playing a role in identifying, notifying, and containing a breach;
- Notifying their supervisor immediately, or, in their absence, the appropriate superintendent or the Freedom of Information (FOI) Officer, upon becoming aware of a breach or suspected breach; and
- Containing, if possible, the suspected breach by suspending the process or activity that caused the breach.

The Board of Trustees is responsible for:

- Ensuring alignment of this administrative procedure with the Records and Information Management Directional Policy;
- Reviewing the Privacy Breach Response Administrative Procedure as part of its regular policy and procedure review cycle.

The Director of Education is responsible for:

- Briefing senior administration and board members as necessary and appropriate;
- Reviewing internal investigation reports and approving required remedial action;
- Monitoring implementation of remedial action; and
- Ensuring that those whose personal information has been compromised are informed as required.

Superintendents, principals, vice-principals, managers and supervisors are responsible for:

- Alerting the FOI Officer of a breach or suspected breach and working with the FOI Officer to implement the five steps of the response protocol;
- Assisting the FOI Officer in obtaining all available information about the nature of the breach or suspected breach, and determining what happened;
- Working with the FOI Officer to undertake all appropriate actions to contain the breach; and
- Ensuring details of the breach and corrective actions are documented.

Freedom of Information (FOI) Officer is responsible for:

- Ensuring that all five steps of the response protocol are implemented;
- Supporting the principal, manager, supervisor and senior administration in responding to the breach; and
- Notifying the Information and Privacy Commissioner where appropriate.

Third-Party Service Providers are responsible for:

- Taking reasonable steps to monitor and enforce their compliance with the privacy and security requirements defined in the contracts or service agreements;
- Informing the board contact or FOI Coordinator of all actual and suspected privacy breaches;
- Documenting how the breach was discovered, what corrective actions were taken and reporting back;
- Undertaking a full assessment of the privacy breach in accordance with the third-party service providers' contractual obligations;
- Taking all necessary remedial action to decrease the risk of future breaches; and
- Fulfilling contractual obligations to comply with privacy legislation.

RESPONSE PROTOCOL:

Unauthorized disclosure of personal information is the defining characteristic of a privacy breach, regardless of whether it was intentional, accidental or the result of a theft or malicious intent.

All privacy breaches or suspected privacy breaches must be reported to the principal or supervisor, or in their absence, to the appropriate superintendent or FOI Officer.

Once reported, the supervisor or superintendent will contact the FOI Officer and the following response steps will be implemented.

Step 1 – Respond

- When a suspected privacy breach is identified by an internal or external source, contact the appropriate department to investigate;
- Assess the situation to determine if a breach has indeed occurred and what needs to be done;
- 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 efforts have been made to contain the privacy breach:

- 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 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, as required, the individuals whose personal information was disclosed;
- Refer to the below section: “How do you Determine if 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 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 about the breach;
- Report the privacy breach to the Office of the Information and Privacy Commissioner (IPC) as appropriate.

How do you Determine if Notification is Required?
Consider the following factors when determining whether notification is required:

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

Risk of Identity Theft
Is there a risk of identity theft or other fraud as a result of the breach? 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 Hurt, Humiliation, or Damage to Reputation
Could the loss or theft of information lead to hurt or 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?

Legislative Requirements (PHIPA, Regulation 329/04)
Notice to Affected Individual:

Under the Personal Health Information Protection Act, a Health Information Custodian (HIC), having knowledge that personal health information in their custody or control was lost, stolen or used/disclosed without authority, is required to:

- Notify the individual of the theft or loss or unauthorized use or disclosure of the individual's personal health information; and
- Include in the notice a statement the individual is entitled to make a complaint to the Information Privacy Commissioner.

Notice to the IPC is required when:

- The HIC has reasonable grounds to believe the personal information in their custody or control was used or disclosed without authority by a person who knows or ought to have known they were using or disclosing the information without authority (example: snooping); or
- The HIC has reasonable grounds to believe personal information in their custody or control was stolen (example: stolen records from car, computer hacking); or
- The HIC has reasonable grounds to believe that, after an initial loss or unauthorized use or disclosure of personal health information in their custody or control, the personal health information was or will be further used or disclosed without authority (example: a subsequent breach could happen from the initial breach); or
- The loss or unauthorized use or disclosure of personal health information is part of a pattern of similar losses or unauthorized uses or disclosures of personal health information (example: an automated process results in similar breaches over time); or
- The HIC determines the loss or unauthorized use or disclosure of personal health information is significant taking into consideration the sensitivity and volume of information, the number of individuals affected, and whether more than one HIC was responsible; or
- The HIC is required to give notice to a College of an event described in section 17.1 of the Act that relates to a loss or unauthorized use or disclosure of personal health information (see Notice to College below).

Notice to the IPC generally is not required if:

- The breach was not intentional; and
- The breach was a "one-off" incident and not part of a pattern; and
- The breach is contained; and
- The scope of the breach was not significant; and

- There are no risks of identity theft, physical harm, hurt/humiliation or damage to reputation, or loss of business or employment opportunities.

Notice to College:

A HIC is required to give written notice to their College within 30 days of the following events:

- An individual they have employed as a HIC who is a member of a College, is terminated, suspended or subject to disciplinary action as a result of the unauthorized collection, use, disclosure, retention or disposal or personal information; or
- The employee resigns and the HIC has reasonable grounds to believe the resignation is related to an investigation or other action by the custodian with respect to an alleged unauthorized collection, use, disclosure, retention or disposal of personal health information by the employee.

Step 5 - Implement Change

When determining what changes and remedial actions need to be implemented, 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.

PROGRESS INDICATORS:

- Mandatory annual privacy training for all staff.
- Statistics about breaches involving a theft, loss, or unauthorized use or disclosure of personal information must be submitted to the IPC as part of the Board's annual statistical report.
-

DEFINITIONS:

Privacy Breach: A privacy breach occurs when personal information is stolen or lost or is collected, used or disclosed without authority.

Personal information: Information about an identifiable or potentially identifiable individual, as defined under privacy legislation.

Third-party Service Providers: Contracted third parties used to carry out or manage programs and/or services on behalf of the board. For the purpose of privacy breach reporting, third party includes all contractors that receive personal information from the board or collect personal information on behalf of the board.

SUPPORTING DOCUMENTS:

- Appendix A: Sample Privacy Breach Report
- 1202 - Protection of Privacy AP
- 1207 – Freedom of Information AP
- Personal Information Management Training Video

REFERENCES:

- *Education Act*
- *Municipal Freedom of Information and Protection of Privacy Act*
- *Personal Health Information Protection Act*