Peterborough Victoria Northumberland and Clarington Catholic District School Board

BOARD ADMINISTRATIVE PROCEDURE	
Administrative Procedure **Protection of Privacy**	Administrative Procedure Number **1202**
Directional Policy **1200 - Records and Information Management**	

Title of Administrative Procedure:

Protection of Privacy

Date Approved:

June 4, 2024

Projected Review Date:

2029

Directional Policy Alignment:

The Protection of Privacy Administrative Procedure aligns with Directional Policy 1200 – Records and Information Management, by articulating the Board's legislative obligations and operational commitment to the protection of personal and confidential information held by the Board.

Alignment with Multi-Year Strategic Plan:

The Protection of Privacy Administrative Procedure supports our Board's Multi-Year Strategic Plan by fostering a culture of privacy that respects the personal, confidential, and sensitive information within the Board's care and control.

PVNCCDSB Board Vision, Mission and Strategic Priorities

Action Required:

The Peterborough Victoria Northumberland and Clarington (PVNC) Catholic District School Board shall comply with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the Personal Health Information Protection Act (PHIPA).

PVNC Catholic is committed to the protection of privacy and recognizes that all employees are responsible for the protection of personal, confidential, and sensitive information entrusted to them.

The collection, use, disclosure, retention, and destruction of personal information shall comply with the provisions of relevant legislation including MFIPPA, PHIPA and the Education Act.

The Board acknowledges that an individual has the right to personal privacy with respect to records in the custody and/or control of the Board.

The Board will establish and maintain a privacy breach protocol.

Collection and Use of Personal Information:

- The Board may collect personal information while fulfilling its mandate.
- The Board will only collect personal information related to the Board's mandate.
- The Board will collect personal information directly from the individual to whom the information relates, except where an exemption under MFIPPA may apply.
- At the time of collection individuals shall be given notice of the legal authority for collection, the purpose(s) of its intended use and the title and contact information of an individual who may respond to specific questions regarding the collection. Individuals will be informed should the purpose for their personal information change.

Disclosure of Personal Information:

MFIPPA sets out when the Board may disclose personal information in its custody and control.

a) <u>Consistent Purpose</u>
Information may be disclosed for the purpose for which it was obtained or compiled or for a consistent purpose provided that the individual about whom the information relates might reasonably have expected such a use or disclosure of the information.

b) <u>With Consent</u>
If the person to whom the information relates has identified that information and consented to its disclosure, that information may be disclosed. When dealing with

minors, it is a best practice to have consent in writing with a signature from the parent/guardian or an electronic sign-off such as an online consent form.

c) Legal Authority
Personal information may be disclosed for the purpose of complying with an Act of the Legislature or an Act of Parliament, an agreement or arrangement under such an Act.

d) Law Enforcement
Personal information may be disclosed to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

e) Health and Safety
Personal information may be disclosed in compelling circumstances affecting the health or safety of an individual. When disclosing information under this section the imminence and reasonableness of the risk to health and safety must be considered and balanced with the invasion of privacy.

f) Performance of Duties
Personal information may be disclosed to an employee, officer, consultant, or agent who needs the record in the performance of their duties and if the disclosure is necessary and proper in the discharge of the institution's functions.

Third Party Contractors and Sharing of Personal Information:

a) The Board enters into agreements with various service providers and contractors for both administrative and educational programs and services. Depending on the nature of the services provided by the contractor, it may be necessary for the contractor to have access to personal information in the Board's custody.

b) Personal information will be shared with a contractor where reasonably required to perform the services for which the contractor has been retained. Personal information will only be used and disclosed in this way where the purpose for the use is the same or reasonably consistent with the purpose for which it was collected.
Where a contractor will have access to personal information in the Board's custody, the Board will ensure that it has agreements in place with the contractor

requiring the contractor to take all reasonable precautions to protect the personal information to which it has access from unauthorized access, use or disclosure.

Third Party Requests for Information:

a) Information will not be disclosed to individual third parties upon request, including legal counsel, without the written consent of the individual to whom the information pertains.

b) Staff must take reasonable care to authenticate the request, which may include contacting the individual to whom the information pertains or requesting identification or credentials.

Privacy Breaches:

a) A privacy breach occurs when personal information is lost, stolen, or subject to unauthorized access or disclosure, contrary to the *Education Act* or *MFIPPA*. This includes the loss of files, computers, personal devices or media that contain personal information.

b) The Board's Privacy Breach Protocol will come into effect upon the awareness of a perceived or actual breach.

Practices for Protecting Personal Information

These practices reflect the Board's commitment to protecting personal information. Employees are expected to follow these practices in the course of their duties.

a) Restrict access to personal information to those employees that require the records and information in the performance of their assigned duties.

b) Ensure that sensitive and confidential information is not visible to the public.

c) Encourage a clean desk policy to reduce the risk of exposing confidential information to others.

d) Lock doors and filing equipment when one's office is not in use.

e) Label filing cabinets, drawers, boxes and other storage containers in a manner that maintains the anonymity of items in storage.

f) Keep open filing equipment or mail boxes behind a counter or other physical barriers to the public.

g) Locate FAX machines and printers in a secure area, and retrieve sensitive documents immediately.

h) Ensure that secure confidentiality is maintained when transporting confidential information (e.g. student assignments or exams home for marking).

i) Ensure records that are the property of the Board, in particular student assignments and exams, are not removed from Board control when an employment contract is terminated.

j) Consult the Board's Records and Classification Retention Schedule or the Records and Information Management Coordinator to determine how long to retain personal information.

k) Ensure confidential destruction of paper records by placing the records in one of the locked shredding boxes for pick up by the shred vendor.

l) Shut down programs or use password protection on computers when leaving work areas.

m) Position computer screens to prevent unauthorized viewing.

n) Notify the appropriate Board personnel when there is a change in an employee's employment status that would affect their access to information.

o) Do not disclose passwords to others.

p) Report any lost or stolen records to your immediate supervisor.

Responsibilities:

The Board of Trustees is responsible for:

- Ensuring alignment of this administrative procedure with the Records and Information Management Directional Policy.

- Reviewing this administrative procedure as part of its regular policy and procedure review cycle.

The Director of Education is responsible for:

- Providing leadership and designating resources to ensure the implementation of and compliance with this administrative procedure.
- Ensuring review of this administrative procedure at regular intervals.
- Authorizing decisions with respect to privacy breach responses.

The Communications Manager is responsible for:

In the role of Freedom of Information and Privacy Officer:

- Overseeing Board compliance with privacy legislation.
- Managing and investigating privacy complaints.
- Establishing, maintaining, and executing a Board Privacy Breach Protocol.

Superintendents, Principals and Managers are responsible for:

- Supporting employees for whom they have supervisory responsibility with the implementation of and compliance with the procedures and requirements under this administrative procedure.
- Implementing reasonable security measures and safeguards to protect personal information.
- Ensuring that agreements with service providers contain privacy protection provisions regarding the protection, collection, use, retention and disclosure of personal information.

Health Information Custodians are responsible for:

- Ensuring confidential management of personal health information in their custody and control as outlined in the Personal Health Information Protection Act.

Staff are responsible for:

- Ensuring they are knowledgeable about the requirements and parameters outlined in this administrative procedure.
- Complying with legislation, professional standards, Board administrative policies and procedures, when using personal information.
- Protecting personal information by following proper procedures and practices as outlined in this administrative procedure and as directed by their supervisor.

- Reporting any suspected privacy or security breaches of which they are aware to their supervisor.
- Taking reasonable steps to ensure the personal information within their custody and control is secured and protected.
- Participating in training regarding their duties and obligations to protect personal information.

Progress Indicators:

- Yearly completion of the Board's annual report to the Information and Privacy Commissioner of Ontario.
- Annual mandatory privacy training module for all Board employees.

Definitions:

Health Information Custodian: Under PHIPA, A health information custodian is an individual who has custody or control of personal health information. i.e. board psychologist.

References:

- MFIPPA
- PHIPA
- AP 1209 – Privacy Breach Response