Niagara Catholic District School Board

PRIVACY POLICY

ADMINISTRATIVE OPERATIONAL PROCEDURES

600 – Business Services **Policy No. 600.6**

Adopted Date: June 20, 2017 Latest Reviewed/Revised Date: December 20, 2022

PURPOSE

The Niagara Catholic District School Board is committed to the protection of personal information under its custody in compliance with its statutory duties and responsibilities. Procedures used in the collection, use, disclosure and retention and security of confidential personal information comply with the *Education Act*, the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) the *Personal Health Information Protection Act* (*PHIPA*) and all other applicable legislation.

SCOPE

The administrative operational procedures apply to all Niagara Catholic employees, trustees, and volunteers who collect, use, retain, disclose, secure and dispose of confidential and personal information pertaining to students and staff on behalf of the Board.

DEFINITIONS

General Information
General information refers to recorded information in the custody or control of the Board that is not of a confidential and personal nature and is not exempt from public access under *MFIPPA* unless an exemption to access applies. Examples of general information that can be released include, but are not limited to, policies and administrative operational procedures, Ministry of Education guidelines and memoranda, travel expense statements, collective bargaining agreements, Board plans, public minutes, or school events and programs.

Personal Information
Personal Information means recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, gender, sexual orientation or marital or family status of the individual,
(b) 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,
(c) any identifying number, symbol or other particular assigned to the individual,
(d) the address, telephone number, fingerprints or blood type of the individual,
(e) the personal opinions or views of the individual except if they relate to another individual,
(f) 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,
(g) the views or opinions of another individual about the individual, and
(h) the name of an individual 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;

Confidentiality
A duty imposed on an organization or individual by laws or professional and ethical standards to restrict access to or disclosure of certain information, which may include personal and/or business information.

The protection of personal information held by the Niagara Catholic District School Board is guided by the principles contained in the Privacy Standard.

Security
"Security/Control" refers to measures designed to protect personal information regardless of media.

PRIVACY PRINCIPLES

Privacy at Niagara Catholic is administered based on the following ten principles:

1. **Accountability and Responsibility**
   The Board has designated the Director of Education as head of Privacy and Freedom of Information for the purpose of the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*). The Director of Education designates the responsibility of duties under *MFIPPA* and the administrative operational procedures of the Privacy Policy to the Board Privacy and Risk Advisor whose accountabilities and responsibilities include:
   - managing the Board Privacy Program;
   - developing, documenting and implementing policies and procedures to protect personal information;
   - managing and overseeing privacy breaches; and
   - providing privacy support and training for all staff.

   Under the *Personal Health Information Protection Act* (*PHIPA)* health information custodians are responsible for personal health information and may designate an individual within the Board as an agent to assist with compliance with privacy legislation.

2. **Identifying Purposes**
   The purposes for which personal information is collected are to be specified, and individuals are notified of the purposes at or before the time personal information is collected.

   Methods to fulfill this principle include the following:
   - Upon information collection, identifying the collection purpose in the Privacy Notice that is included on/in the manner of collection (paper form, electronic form, website);
   - Limit collection to whom the personal information relates; and
   - Obtain consent when a new purpose of collection is identified.

3. **Consent**
   Informed consent is required by an individual for the collection, use, and disclosure of personal information, except where otherwise permitted by law. An individual providing consent must understand the purpose of the consent, to what they are consenting, and that their consent may be withdrawn at any time.

   Methods to fulfill this principle include the following:
   - That sufficient detail will be provided on the collection form so that it is clear to an individual to what they are consenting;
   - That the collection form will identify which parties personal information is being shared;
   - That consent is obtained again when a new use of existing personal information is identified; and
   - That individuals will be informed of the implications of withdrawing consent.

Consent is provided in two different forms, express and implied. Express consent should be obtained in the following circumstances:

- the information being collected, used or disclosed is sensitive
- the collection, use or disclosure is outside of the reasonable expectations of the individual; and/or
- the collection, use or disclosure creates a meaningful residual risk of significant harm.

4. Limiting Collection

The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.
Methods to fulfill this principle include the following:

- Collect only the personal information needed that fulfills an identified purpose;
- Be open and transparent about the reasons for collection, which is captured in the Privacy Notice that is included on Board forms.

5. Limiting Use, Retention, and Disclosure

Personal information can only be used and disclosed for the identified purposes for which it was collected, and must be kept for only as long as it is needed to serve those purposes except where otherwise permitted by law.

Methods to fulfill this principle include the following:

- Any new use of personal information must be documented;
- Employee access to personal information should be limited to what they need for their role;
- Information retention periods should be followed, as per the Records and Information Management Classification System and Retention Schedule;
- Disposal of information that has no specified purpose or no longer fulfills the purpose for which it was collected; and
- Ensure that information is deleted prior to disposal of devices containing digital information.

6. Accuracy

The Board shall ensure that personal information is accurate and complete, and is updated in order to fulfill the specified purposes for its collection, use, disclosure, and retention.

Methods to fulfill this principle include the following:

- Allow staff and students to have their personal information updated annually and as required.

7. Security Safeguards

The Board shall take all steps necessary to ensure that personal information is secured and protected from unauthorized access, disclosure, use, or modification or inadvertent loss or destruction.

Methods to fulfill this principle include the following:

- Maintain security safeguards including but not limited to:
- Organizational controls such as a clean desk policy, shredding practices, visitor sign-in, end of day procedure (log-out, clear desk);
- Physical controls such as locked cabinets/doors, restricted access to certain locations, surveillance cameras, building security;
- Information technology controls such as user authentication, computer time-outs, anti-phishing software, encryption, firewalls, anti-virus protections;
- Follow the record retention requirements as stated in the Records and Information Management Classification System and Retention Schedule;
- Utilize official document shredding organizations to securely destroy personal information that has met retention requirements.

When working outside of the office, staff should employ the following safeguards:

- Store paper files in a safe and secure location at all times;
- Board documents that contain personal and/or confidential information should always be created on Board-issued devices. If personal mobile and/or electronic devices (including home computers) are used, staff are to ensure that they are password-protected;
- Employees should only use licensed software or applications that have been approved by the Board Information Technology department;
- Never leave a computer unattended with personal information in view.

8. Openness and Transparency

The policies and procedures of the Board relating to the management of personal information shall be made readily available to the public.

Methods to fulfill this principle include the following:

- Posting relevant documentation on the Board public website, and
- Ensure front-line staff are aware of the existence and location of documentation so they can direct stakeholders to it if necessary.

9. Access and Correction

The Board shall permit an individual access to any personal information about them which is held by the Board in accordance with the provisions of the *Education Act* and *MFIPPA*. An individual is entitled to challenge the accuracy and completeness of their personal information held by the Board and may request that it be amended.

Methods to fulfill this principle include the following:

- Should someone request of the Board what personal information is held about them the Board should advise without hesitation, and no later than 30 days;
- Assist people in their preparation for making the request for information (ensure they are able to provide as much information as possible that would enable the Board to locate personal information);
- Where appropriate send revised information to third parties that have access to the information.

10. Compliance

An individual must be allowed to challenge or make a complaint regarding the Board compliance with the above principles. The challenge will be addressed by the role in the Board that is accountable for Privacy.

Methods to fulfill this principle include the following:

- Acknowledge receipt of and accurately record the date and details of the challenge;
- If necessary ensure the challenge is assigned to someone with the skills and knowledge to assess it objectively;
- Upon completion of the challenge, promptly notify the person who initiated the challenge, informing them of the outcome.

ROLES AND RESPONSIBILITIES

- The Board Privacy and Risk Advisor has the overall responsibility for the Board Privacy program and facilitation of Freedom of Information requests.
- All employees, trustees, and third party contractors who collect, use, and retain personal information must adhere to the Privacy principles documented in the administrative operational procedures. They must be aware of and understand their responsibilities to protect personal information while executing their daily duties.
- All employees and trustees are expected to be aware of and adhere to privacy responsibilities noted in other Niagara Catholic Board Policies and Administrative Operational Procedures

including but not limited to the OSR AOP (301.7), the Video Surveillance AOP (701.3), and the Criminal Background Check AOP (302.6.7).

FREEDOM OF INFORMATION REQUEST

In accordance with *MFIPPA* every person has a right of access to a record or a part of a record in the custody of the Board. The Board will make every effort to respond within 30 days after receiving the written request.

- A request must be made in writing using the *Freedom of Information Request Form*.
- A request must provide sufficient details to enable the Board to identify and locate the record.
- Upon submission of the Freedom of Information Request Form, a fee of $5.00 must be remitted.
- A request that is deemed frivolous or vexatious will not be granted.

Additional details are provided in the *Freedom of Information Request Protocol*.

NIAGARA CATHOLIC PRIVACY BREACH PROTOCOL

A privacy breach is the loss of, unauthorized access to, disclosure of, or destruction of, personal information. In the event of a privacy breach or suspected breach, employees will immediately notify their Supervisor and follow the steps outlined in the *Privacy Breach Protocol*.

Adopted Date:	**June 20, 2017**
Revision History:	**December 20, 2022**