HALTON CATHOLIC DISTRICT SCHOOL BOARD

Procedure No. VI-81

Privacy Procedure

Adopted:	**Last Reviewed/Revised:**
October 31, 2016	December 2, 2024

Next Scheduled Review: 2027-2028

Associated Policies & Procedures:

I-07 Protection of Privacy
VI-51 Security Breach Procedure
I-02 Records and Information Management Policy
VI-82 Records and Information Management Procedure
I-30 Video Surveillance
VI-83 Video Surveillance Procedure
I-43 Use of Technology and Digital Citizenship
VI-62 Use of Technology and Digital Citizenship
VI-63 Social Media
II-38 Educational Research
VI-25 Educational Research
V-18 Community Engagement and Public Consultation Policy
I-46 Trustee Communications and Correspondence to Board

Purpose

To ensure the protection of personal information collected, used, retained, and disposed of by the Halton Catholic District School Board (HCDSB) is in compliance with the *Education Act*, the *Municipal Freedom of Information and Protection of Privacy Act*, (MFIPPA), *the Personal Health Information Protection Act* (PHIPA), *the Personal Information Protection and Electronic Documents Act (PIPEDA)* and any other applicable legislation.

This procedure establishes guidelines for safeguarding privacy, ensuring alignment with technical measures outlined in *VI-101 Information Security Procedure*, to protect personal information under HCDSB's custody or control.

Application and Scope

This procedure applies to all HCDSB employees, Trustees, and third party service providers who collect, use, retain, and disclose personal information pertaining to students and/or HCDSB employees. It governs, operations and activities conducted within all HCDSB facilities and extends to

the use of technology and digital and social media platforms, ensuring alignment with the technical safeguards and protocols outlined in *VI-101 Information Security Procedure*.

Principles

HCDSB is committed to protecting the privacy of individuals by ensuring the secure collection, use, retention, and disposal of personal information in compliance with the Education Act, MFIPPA, PHIPA, PIPEDA and any other applicable privacy legislation.

HCDSB adheres to the following 9 Privacy Principles:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection, Use, Disclosure and Retention
5. Accuracy
6. Safeguards
7. Openness
8. Individual Access and Correction
9. Challenging Compliance

Requirements

1. Accountability

The Director of Education is accountable for the action taken and decisions made under MFIPPA and ensures there is oversight of and compliance with the privacy policy and procedures and may appoint a staff designate who shall, pursuant to applicable legislation be responsible for:

- Administering and ensuring compliance with respect to the collection, use, disclosure and retention of personal information;
- Ensuring that procedures are in place regarding third party service providers who have custody of personal information on behalf of the HCDSB.
- Processing of all Freedom of Information Request, appeals, mediation
- Managing the process for the correction of personal information
- Managing and overseeing privacy breaches
- Communicating and providing training opportunities to employees

2. Identifying Purposes

The HCDSB only collects personal information when it is necessary for providing for the education for students and/or the employment of HCDSB employees, or as required and authorized by law.

The HCDSB has adopted the following practices to standardize how it collects personal information and personal health information:

- Personal information, including health information managed by regulated health professionals in their role serving as Health Information Custodians, will only be collected for a specified purpose, noting the legislative authority for the collection;
- When collecting personal information:
    - collect personal information directly from the individual to whom it relates. If using an indirect or alternative manner of collection, employees must adhere to the specific provisions stipulated in MFIPPA and PHIPA;
    - Make every attempt to ensure the accuracy and integrity of personal information and collected;
    - Obtain, prior to collection, the necessary consents;
    - When collecting information on forms, websites or through surveys there must be a disclaimer which indicates the legal authority for the collection of the information, purpose(s) for which the personal information is to be used; and provide the contact information of the appropriate staff position that will be able to answer questions regarding the collection.
- On an annual basis the HCDSB will provide notice to parents/guardians and students regarding the Routine Collection, Use and Disclosure of Student Personal Information. See Appendix A.

3. Consent

The HCDSB will seek consent, if required, for the use or disclosure of personal information and/or personal health information at the time of collection.

- When an individual has been informed of the purpose of collection, use, or disclosure they can give consent in many ways, for example:
    - Using a paper or electronic form to provide explicit, written consent. By completing and signing a form, or by clicking a checkbox and pressing the submit button the individual provides their consent to the collection and the specified uses. Email or other verifiable electronic correspondence may also be used.
    - If obtaining written consent is impractical, oral consent in these limited circumstances, such as telephone communication, may be used. It, will be accepted if date and time, full name of individual and short description of conversation are recorded. For example, "On [date], [name] gave oral consent to disclose [specific information] to [recipient] for [purpose]."

Withdrawal of Consent

An individual may withdraw consent at any time.

- The HCDSB will inform the individual of the implications of such a withdrawal;
- Document date and time, individual's name and details of the withdrawal. For example, "Consent to disclose [information] was withdrawn on [date]."
- If an individual withdraws their consent the HCDSB will stop collecting, using, disclosing or retaining information upon receipt of the withdrawal of consent, or abiding by the directions of the individual in the case of variation of consent.

4. Limiting Collection, Use, Disclosure and Retention

The HCDSB will comply with legislation that restricts the use of personal information to the purpose for which it was collected, a consistent purpose, purposes to which the individual consents and other limited circumstance:

The HCDSB will only retain records containing personal information in accordance with the HCDSB's Retention Schedule and for the period stated in the appropriate privacy legislation;

The HCDSB will make an informed decision considering all relevant circumstances before disclosing the personal information;

a. These considerations will include whether the disclosure is in the interest of the individual(s) and whether the disclosure is necessary for providing for the education of students or administering the employment of HCDSB employees. Consequently, disclosure of personal information is only provided to employees and third party service providers who require this information to perform their duties.

b. When the HCDSB receives requests for personal information from the Ministry of Education, other ministries, other Ontario school boards/authorities or private agencies, they will verify the legal authority for the disclosure

5. Accuracy

a. The HCDSB will routinely request personal information to be updated.

6. Safeguards

To protect the personal information within the custody and/or control of the HCDSB follow these best practices:

- Restrict access to personal information to only those employees requiring access in order to carry out their duties;
- Do not disclose personal information to any member of the public, the HCDSB, Trustees, or other employees without the consent of the individual to whom the information relates, or in accordance with legislation;
- Do not discuss personal matters pertaining to any employee or student in public areas where it may be overheard by others who are not otherwise authorized to have such information;

- Do not leave personal information exposed or visible on desks or on computer screens. Employees should lock computer screens and put physical records containing personal information away in a secure location when it is not in use;
- Do not remove records and files containing personal information from HCDSB worksites, unless required to complete duties and responsibilities of the position, for example, the marking of tests;
- Do not share, post or disclose system, software and email passwords allowing unauthorized users access to personal information;
- Apply confidentiality and privacy statements to all email, fax transmissions and documents that contain personal information;
- Secure all cabinets or storage locations containing personal information and/or personal health information at the end of each day or when not in use.
- Dispose of personal information utilizing secure methods, such as shredding, to maintain confidentiality of the information,
- Encrypt devices containing Personal Health Information.
- Upon resignation from the HCDSB or transfer to another location, all files containing personal information on employees in paper or electronic format at the site level will be destroyed, if applicable.
- All parent/guardian personal information provided to a Catholic School Council for purposes of supporting parent engagement will be returned to the principal at the end of the school year and destroyed, if applicable.
- The HCDSB will monitor the implementation of security safeguards and privacy risk management by employees and third-party service providers by conducting periodic checks and other measures.
- Identifiable threats to safeguarding personal information will be addressed and alternate practices put in place.

7. Openness

- Policies and practices relating to the management of personal information are made readily available to the public.

8. Individual Access and Correction

Access

- The public has a right of access to information of a publicly funded institution.
- Access to information can be handle through routine disclosure and active dissemination of information for general HCDSB information.
- Access to information may also be handled through the formal access to information request process.

- An individual has the right to personal privacy with respect to records in the custody and/or control of the HCDSB.

Correction

- When an individual successfully demonstrates the inaccuracy or incompleteness of personal information or personal health information, the HCDSB will amend the information as required.
- Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information.
- Where appropriate, the amended information will be transmitted to third party service providers having access to the information in question.

9. Challenging Compliance

- An individual has the ability to address or challenge compliance with the above principles to the Director of Education and the Office of the Information Privacy Commissioner.

Privacy and Social Media

1. Any information shared via the HCDSB's social media accounts are subject to the provisions of MFIPPA. This means that social media information may be accessed and disclosed in response to an access request under MFIPPA, or a legal proceeding.
2. To protect their own privacy and the privacy of others, employees should not include personal information in comments or any other content posted within a Social Media account registered to the HCDSB. Personal information includes home addresses and telephone numbers, photographs containing images of identifiable individuals, and any other information consisting of personal information as defined in the Act.
3. Prior to the posting of student work, names, photos, or video of students, ensure parents/guardians have consented to sharing this information.

Responsibility

Trustee(s) Own Records

The provisions of MFIPPA cover records that are in the custody or under the control of the HCDSB. This includes information created by a third party that has been provided to, or obtained by, the Trustee(s). Trustee(s) records are subject to MFIPPA if they are related to the discharge of the Trustee(s) responsibilities as a member of the HCDSB.

Superintendents, Administrators, Managers and Supervisors

Superintendents, Administrators, Managers and Supervisors shall be responsible for overseeing the collection, use, and routine disclosure of information and records associated within their area of responsibility. This includes:

1. Administering all requests for access to **general non-confidential** information in accordance with MFIPPA;

2. Ensuring all personal information is managed and protected in accordance with the privacy policy and procedure and all applicable privacy legislation and Ministry guidelines;
3. Providing ongoing communication of the privacy policy and procedure to all employees;
4. Ensuring programs and services within their service area integrate protection of personal privacy requirement into the development, implementation, evaluation and reporting activities;
5. Promoting a culture and business practices that ensures HCDSB information is shared and accessible to the greatest extent possible while respecting the security and privacy requirements of personal information. This includes the use of third-party data sharing agreements when personal information is shared beyond the HCDSB or with agents of the HCDSB.

Manager, Privacy, Records and Information Management Services

The Manager, Privacy, Records and Information Management Services will be designated by the Director of Education, as the individual to oversee compliance of MFIPPA and PHIPA legislation.

1. Develop and implement policies, programs and services for the management and protection of personal information based on MFIPPA, PHIPA, Education Act, and the Ontario Student Record (OSR) guidelines.
2. In partnership with Superintendent, Administrators, Managers and Supervisors of Departments and programs, ensure implementation of this policy and review practices for collecting and managing personal information holdings at the HCDSB;
3. Consult with employees to meet privacy requirements as identified in the privacy policy and procedures, applicable legislation, and privacy standards;
4. Ensure proper notice is given and the required level of consent is obtained (as required) prior to the collection of all personal information;
5. Coordinate the response to complaints regarding the misuse of personal information;
6. Investigate reports of privacy breaches;
7. Sign-off and execute recommendations of any Privacy Impact Assessment (PIA) report prior to implementation of technology, system, program or service involving the collection or use of personal information;
8. Develop guidelines, training material and other tools as required to assist employees and the public on matters pertaining to the collection, use and disclosure of personal information;
9. Ensure that adequate disposal processes for personal information are in place and adhered to;
10. Be responsible for the receipt, coordination of responses for all formal access requests received pursuant to MFIPPA in collaboration with all Departments and Program Areas;
    a. Official requests for access to information will be directed to the Manager, Privacy, Records, and Information Management Services for registration, documentation and receipt acknowledgement;

b. A copy of all requests will be directed to the Director of Education or designate for information and to the appropriate supervisory officer for response;

c. All responses will be forwarded to the Manager, Privacy, Records, and Information Management Service for review, final documentation and dispatch to the requestor;

d. Any delay in preparing a response within thirty (30) calendar day limit, as noted in MFIPPA, will be promptly forwarded to the Manager, Privacy, Records, and Information Management Service, to ensure appropriate notice is given to the requestor and in accordance with MFIPPA;

e. Where permissible request processing fees are estimated to exceed $25.00, a cost estimate will be sent to the Manager, Privacy, Records, and Information Management Service, for the appropriate action.

11. Assist the public with requests for access to information as required.

Senior Manager, Information Technology

The Senior Manager, Information Technology shall be responsible for:

1. In collaboration with the Manager, Privacy, Records and Information Management Services, implement Privacy and Information Management principles in Enterprise Architecture, Information Technology policies, standards, procedures and technologies where appropriate;
2. Create personal information privacy and security standards for technologies that will ensure adequate safeguards and compliance for those technologies or technological processes that collect, use, disclose or retain personal information and/or personal health information;
3. Conduct Risk Assessments (such as Privacy Impact Assessments Threat Risk Assessments and Vulnerability Assessments) on technological systems involving the collection or use of personal information or personal health information to implement or deployment.

Employees

Employees shall be responsible to:

1. Understand their responsibilities to protect privacy in executing their operational duties;
2. Ensure responsibility for the privacy of the HCDSB business information regardless of the technology used to manage the information;
3. Be aware of and adhere to their privacy responsibilities noted in the HCDSB's *I-43 Use of Technology and Digital Citizenship Policy*;
4. Be aware and adhere to their privacy responsibilities noted in *I-30 Video Surveillance Policy*;
5. Make every reasonable attempt to ensure that all personal information collected is accurate, complete and up-to-date;
6. Assist the public with requests for access to information and disclosure of routine records and information (where appropriate) that are within their scope of responsibility;

7. Adhere to the disposal requirements contained in this and other records management policies and procedures of the HCDSB.

APPROVED: Regular Meeting of the Administrative Council

AUTHORIZED BY: _____

Director of Education and Secretary of the Board

APPENDIX A

NOTIFICATION OF THE ROUTINE COLLECTION, USE AND DISCLOSURE OF STUDENT PERSONAL INFORMATION

This document must be sent home annually and posted on the HCDSB and school websites.

The Halton Catholic District School (HCDSB) wants parents/guardians to understand how we use and disclose student personal information that is collected pursuant to our obligations set out in the Education Act and in accordance with the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).*

The Education Act authorizes school boards to collect personal information, for planning and delivering educational programs and services which best meet students' needs and for reporting to the Minister of Education as required. The "Act" also requires that the school principal maintain an Ontario Student Record (OSR) for each student attending the school. The OSR is a record of a student's educational progress throughout school in Ontario and follows students when they transfer schools.

Under the MFIPPA, personal information may be used or disclosed by HCDSB:

- For the purpose for which it was obtained or a consistent purpose (a purpose consistent for the reason collected).
- To HCDSB officers or employees who need access to the information in the performance of their duties if necessary and proper in the discharge of the HCDSB's authorized functions.
- To comply with legislation, a court order or subpoena or to aid in a law enforcement investigation conducted by a law enforcement agency; and, in compelling circumstances affecting health or safety (providing notice of the disclosure is sent to the student's home).

The following are routine collection, uses and disclosures of student personal information:

1. Student personal information, including the OSR will be used by authorized school and HCDSB employees for developing an educational program which best meets the student's needs.
2. Information about the student may be shared between both elementary and secondary schools to support the transition of the student.
3. Secondary schools will share information about student progress throughout secondary school with the students' previous elementary school to support continuous improvement of the elementary school program for all students.
4. Student personal information such as home address, photo, life-threatening medical emergency information, accessibility and safety needs and emergency contact information will be released to the Halton Student Transportation Services (HSTS) and the contracted bus companies responsible for transporting students in order to administer theHCDSB's contracted transportation program.

5. Student accidents that take place during school or on school-sponsored activities will be reported to the HCDSB insurer. Reports include the name of the injured student(s) and details about the incident as well as the name and contact information of witnesses to the accident.
6. Student information may also be shared with the Region of Halton Public Health Dept. in accordance with the Immunization of School Pupils Act. Please note that communicable diseases (e.g., Measles, Tuberculosis) are reported in accordance with the Health Promotion and Protection Act. Limited student information related to violations of the Smoke Free Ontario Act may also be reported to the Public Health Department.
7. Student information may also be shared with the Halton Children's Aid Society as required by law.
8. Student information may also be shared with medical responders and/or the hospital, when responding to a medical emergency.
9. Phone numbers will be used on emergency telephone lists. Examples include emergency contact lists to facilitate contact with parents/guardians during emergencies (e.g., inclement weather & safe arrival programs), which may be staffed by parent/guardian volunteers, to contact parents/guardians when a student is absent, and the parent/guardian has not notified the school of the absence.
10. Information may be used to deal with matters of health and safety and may be required to be disclosed in compelling circumstances, or for law enforcement matters.
11. Student work, including student names, may be displayed in the classroom or in school hallways, or may be shared with the public through science fairs, school and HCDSB newsletters, writing/coloring/poster contests, community events, fairs, school programs, brochures, celebration of sacraments and similar events/locations outside the school setting, with consent.
12. Birthday congratulations may be announced over the PA system and/or in the classrooms, in elementary schools.
13. Students may be recorded or photographed by their classroom teacher in school or during school activities, as part of their educational program and for assessment purposes with appropriate consent.
14. Contracted photographers will take individual and class photos of students. These photos along with student names will be used for administrative and archival purposes, on student cards, in school yearbooks and will be offered to parents/guardians for purchase.
15. Limited student information will be provided to the Local or Provincial Athletic Associations for sports team eligibility (e.g. HCAA, GHAC, OFSAA, BYSC) when the student joins a sports team.
16. Secondary schools will send marks, transcript and contact information regarding potential graduates to Ontario application centers for both College and University to support the post-secondary application process.
17. Student names and/or photographs may be printed in school programs (e.g. commencement or graduation programs, school plays and musical productions, student awards, academic and

athletic awards and plaques, school brochures, honour roll and classroom assignments) and in school yearbooks (print & digital) with the appropriate consents.

18. Video surveillance equipment may be used in schools and on HCDSB provided bus services to enhance the safety of students and employees, to protect property against theft or vandalism, and to aid in the identification of intruders.
19. Indigenous ancestry information of First Nation, Métis and Inuit students who chose to voluntarily, self-identify will be used to allocate resources, improve student learning and student success, and to offer individualized supports and opportunities to students and families. Indigenous information will also be reported to the Ministry of Education and the Education Quality Accountability Office (EQAO).
20. Student names, date of birth, student number and classroom are shared with School Cash Online, so parents/guardians may remit payment for student activities electronically.
21. As part of the HCDSB's commitment to 21st century learning, students, with the supervision of the classroom teacher, will be using Ministry and HCDSB approved tools in the classroom. Within these environments, students may use wikis, blogs, podcasts, video conferencing and surveys. The HCDSB supports the following tools; G-Suite for Education, Desire to Learn (D2L), Microsoft Office 365, My Blueprint, and School Messenger.
22. Students will be provided with a HCDSB email account in accordance with HCDSB guidelines.
23. If appropriate, information will be shared with the HCDSB's newcomer Welcome Centre, Interpreters and Settlement Workers.
24. As required by the Personal Health Information Protection Act (PHIPA) and Education Act, parental/guardian consent will be sought prior to the involvement of child and youth counselors, social workers, psychological, behavioral and/or speech and language staff.
25. In accordance with MFIPPA, PHIPA and the Education Act, releasing personal information for any other purpose requires the informed consent of:
    - the parent/guardian for children under 16 years of age;
    - the parent/guardian and the student where the student is 16 and 17;
    - the student where the student is over 18
    - or is 16 or 17 years of age and has withdrawn from parental/guardian control.

If you have any concerns regarding how we collect, use and disclose personal information, please contact HCDSB's Privacy Office at privacy@hcdsb.org.