HALTON CATHOLIC DISTRICT SCHOOL BOARD

Policy No. I-47

Information Security

Adopted: February 8, 2022	**Last Reviewed/Revised:** September 16, 2025
Next Scheduled Review: 2028-2029	
Associated Policies & Procedures: **VI-81** Privacy Procedure **I-02** Records Information Management **I-07** Protection of Privacy **I-30** Video Surveillance **VI-83** Video Surveillance **I-43** Use of Technology and Digital Citizenship **VI-62** Use of Technology and Digital Citizenship **VI-63** Social Media **VI-51** Security Breach Procedure **VI-101** Information Security Procedure **VI-103** Electronic Monitoring of Employees	

Purpose

To outline the requirements to protect the confidentiality, integrity, and availability of Halton Catholic District School Board (HCDSB)'s information.

Application and Scope

This policy applies to all employees, third parties and Trustees with access to HCDSB systems. HCDSB will be risk-focused, comprehensive, and responsive in meeting its cyber and data security commitment

References

Child, Youth and Family Services Act, 2017, S.O. 2017

EC-Council Certified Chief Information Security Officer Program, Version 3

Education Act

Enhancing Digital Security and Trust Act, 2024 (EDSTA)

Evidence Act, R.S.O. 1990, c. E.23

Gartner Glossary

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

National Institute of Standards and Technology Resource Centre

OASBO Privacy and Information Management toolkit (2018)

Ontario Student Record (OSR) Guideline, 2000 (revised 2020)

Personal Health Information Protection Act, 2004

R.R.O. 1990, Reg. 823

Safe Schools Code of Conduct

Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024

Definitions

1. **Artificial Intelligence (AI) System:** automated systems used for decision-making requiring ethical governance under EDSTA.
2. **Cyber Incident**: unauthorized access, disruption, or destruction of information systems (per EDSTA).
3. **Cybersecurity**: is the combination of people, policies, processes, and technologies employed by an enterprise to protect its information assets.
4. **Information Governance (IG):** is the security, control, and optimization of information.
5. **Personal Information (PI):** as defined in MFIPPA, any recorded information about an identifiable individual (e.g., student records)
6. **Privacy Impact Assessment (PIA):** a review that identifies and evaluates how a project or initiative may affect the privacy of individuals and the security of their personal information, and recommends measures to reduce any risks.
7. **Risk Tolerance:** the amount of risk HCDSB is willing to accept before acting or investing in risk mitigation.

Principles

HCDSB acknowledges the practical necessity and the importance of establishing and maintaining a comprehensive information security program conforming to the following Guiding Information Governance Principles:

1. **Accountability:** The Director of Education oversees the HCDSB's Information Security program and designates authority to appropriate individuals as required.
2. **Availability:** HCDSB's Information Security program will be constructed so the information assets generated by or managed for the HCDSB have a reasonable guarantee, timely, efficient, and accurate retrieval.
3. **Compliance:** HCDSB's Information Security program will be constructed to comply with relevant legislation and other information management standards.
4. **Confidentiality:** HCDSB's Information Security program will be constructed so the information assets generated by or managed for the HCDSB have a reasonable guarantee of protection.
5. **Disposition**: HCDSB's RIM program will provide secure and appropriate disposition for information assets no longer required to be maintained, in compliance with applicable laws and the organization's policies.
6. **Ethical Use of Artificial Intelligence:** where Artificial Intelligence (AI) systems are used for decision-making, the HCDSB will apply its Board-approved AI Guidelines to ensure transparency, accountability, ethical governance, and compliance.
7. **Integrity:** HCDSB's Information Security program will be constructed so the information assets generated by or managed for the HCDSB have a reasonable guarantee of authenticity.
8. **Protection of Children's Digital Information:** HCDSB will apply heightened safeguards to protect the digital information of children and youth, consistent with EDSTA and other applicable regulations.
9. **Retention**: HCDSB's Records Information Management (RIM) program will maintain its information assets for an appropriate time, considering its legal, regulatory, fiscal, operational, and historical requirements.
10. **Security & Risk Management:** HCDSB's Information Security program will include proactive risk assessment, implementation of administrative, technical, and physical safeguards, and continuous monitoring to address evolving cybersecurity threats.
11. **Transparency:** HCDSB's processes and activities, including its Information Security program, will be documented in an open and verifiable manner and available to all authorized personnel and appropriate interested parties.

Requirements

If you are an employee, third party or Trustee, you must:

1. Take the required steps to protect the confidentiality, integrity, and availability of HCDSB information prescribed in HCDSB procedure *VI-101 Information Security* and all HCDSB associated policies and procedures.

2. Comply with legal and regulatory requirements, specifically the *Municipal Freedom Information Protection Privacy Act* and the *Enhancing Digital Security and Trust Act, 2024 (EDSTA)* where applicable.
3. Take all mandatory security training.
4. Participate in regular cybersecurity awareness refreshers as part of the HCDSB's compliant cybersecurity program.
5. Conduct PIAs for all projects involving PI collection/use.
6. Implement and maintain a Board-wide cybersecurity program that includes risk assessments, administrative, technical, and physical safeguards, continuous monitoring, and regular updates to address evolving threats.
7. Maintain an incident response plan that includes detection, response, documentation, reporting of significant breaches, and post-incident reviews to improve controls.
8. Where Artificial Intelligence (AI) systems are used for decision-making, follow the HCDSB's AI Guidelines to ensure transparency, accountability, and ethical governance.
9. Apply heightened safeguards to protect the digital information of children and youth.

Employees, third parties and Trustees are required to comply with this policy. Any activities causing a security incident may lead to disciplinary action, including the issuance of a verbal or written warning followed by additional training on security for a minor incident, up to and including termination in the case of a major and/or intentional incidents.

Each disciplinary matter will be examined on a case-by-case basis.

Responsibilities

Effective information security management is critical to the operation of all HCDSB sites and is the responsibility of every employee, third party or Trustee.

1. **Director of Education:** is accountable for ensuring there is an information security program that complies with the principles of information governance, including determining the HCDSB's risk tolerance and the required resources to ensure ongoing compliance, as well as integrating security processes into operational and strategic planning.
2. **Senior Manager, Information Technology Services:** is responsible for ensuring all boundary and internal network protection controls are established and maintained, as well as cybersecurity oversight as outlined in EDSTA.
3. **Management and Administrators:** all managers must oversee compliance with and enforce this policy, including ensuring staff have signed off on the review of this policy.
4. **Employees, Third Parties and Trustees:** all employees, third parties and Trustees must comply with this policy.

APPROVED: Regular Meeting of the Board

AUTHORIZED BY: _____

Chair of the Board