Halton District School Board

Cyber Security and Data Protection

Board Policy

Adopted: **January 2024**
Revised: **March 2024**
Review Date: **January 2025**

Objective

This policy establishes the framework for the protection of critical information, the management of cyber risks, and the mitigation of cyber threats to:

- Personal Information (PI), Personal Health Information (PHI) and other board sensitive information;
- Board information systems, network(s) and sub-network(s) and devices;
- education technology applications and tools;
- internet connected equipment used in the management of board facilities; and
- staff and students when online and using board-provided technology, devices, and/or network(s) or sub-network(s).

Policy Statement

The Board is committed to facilitating the secure, safe, responsible and respectful use of technology to support teaching and learning, to prepare students for the risks and opportunities of the digital world, and to ensure students thrive safely online and become good digital citizens. Specifically:

a) The Board's Cyber Security and Data Protection Policy and Administrative Procedure shall comply with all applicable laws, legislations and Ministry of Education policy directives.

b) The Board is committed to adhering to the requirements of the provincial Cyber Security Wellness Architecture (CSWA) and the standards set out in the NIST Cybersecurity Framework 2.0 Core and Security Reference Architecture (RA) 3.0.

c) Comprehensive Board standards, procedures and guidelines for cyber security, cyber safety and the protection of online privacy shall be developed, implemented, communicated and maintained up to date in accordance with the direction and priorities established by the Board.

d) The Board shall establish and maintain a multi-year plan for implementing and improving cyber protection in the Board.

e) The Cyber Security & Data Protection Policy and Administrative Procedure shall include clear accountability and responsibility for cyber protection (cyber security, cyber / online safety and online / digital privacy) in the Board.

f) Authorized users shall comply with the Board's Cyber Security & Data Protection Policy and Administrative Procedure and all associated standards, procedures and guidelines, as applicable.

Responsible use of technology is further defined in and governed by the Board's Responsible Use of Information and Communication Technology (ICT) Administrative Procedure.

Scope

This Policy applies to all staff, students, vendors, contractors, and consultants, who create, distribute, access, or manage information by means of the HDSB's information systems including personal or corporate computers, networks, and communication services by which they are connected. It equally applies to individuals and enterprises, who by nature of their relationship with the HDSB, are entrusted with confidential or sensitive information.

Guiding Principles

The Halton District School Board (HDSB) recognizes digital information, information systems, education technology and internet connectivity as integral parts of the Board's K-12 education system. They are essential in day-to-day operations,

administrative functions and facilities management while enhancing and enriching teaching and learning in school and during periods of remote learning.

The HDSB also recognizes its responsibility in the stewardship of information technology, digital resources, and the security of sensitive information that is stored on Board information systems.

To deliver on the requirements of this policy, the Board recognizes the importance of adopting a comprehensive approach to cyber protection that includes, but is not limited to:

- **Cyber Protection Governance** to prioritize and inform key decisions, have clearly defined accountability for cyber protection in the Board, and ensure all key stakeholders are represented to ensure the board's technology ecosystem is protected;
- **Cyber Protection Strategy / Roadmap** which defines the HDSB's plan to improve cyber protection in the HDSB and its overall approach to managing cyber risks to the HDSB's K-12 technology ecosystem and its users;
- **Cyber Protection Tools, Standards, Procedures and Guidelines** which defines specific mandatory or recommended measures (also commonly referred to as safeguards or "rails") to defend against cyber threats, producing a reliable foundation for cybersecurity, cyber safety, and privacy protection for the HDSB and its staff and students; and
- **Cyber Protection Assurance** which refers to continually assessing the adequacy and efficacy of cyber protection measures in protecting the HDSB and its staff and students from current and evolving cyber threats.

Terminology

Cyber Protection

Term used to collectively describe the following three areas: Cyber Security, Cyber / Online Safety and Digital / Online Privacy

Halton District School Board

Cyber Security and Data Protection

Board Policy

Cyber Security (also: "Cybersecurity")

The protection of I&IT resources with respect to confidentiality, availability and integrity as well as secure network-connected OT resources

Cyber / Online Safety

The promotion of safe online practices and the mitigation of the risk involved with the inappropriate use of technology in accordance with the Board's Responsible Use of ICT Administrative Procedure

Digital / Online Safety

The protection of Personal Information (PI), Personal Health Information (PHI) and other board sensitive information from unauthorized access and the recognition of the importance of guarding personal and sensitive information when using technology

I&IT

Information and Information Technology

OT

Operational Technology used by vendors, third parties, etc. to connect to the Board's network(s) and/or sub-network(s) and includes the Industrial Internet of Things (IIoT) / Internet of Things (IoT), HVAC systems, building sensors, key scan cards, and more

Halton District School Board

Cyber Security and Data Protection

Board Policy

Related Board Policies

Privacy and Information Management Policy
Risk Management Policy

Related Board Administrative Procedures

Board Assigned Mobile Cellular Device Administrative Procedure
Cyber Security and Data Protection Administrative Procedure
Privacy Breach Protocol Administrative Procedure
Records Management Administrative Procedure
Responsible Use of Information and Communication Technology (ICT) Administrative Procedure
Risk Management Administrative Procedure
School, Staff, and Student Websites Administrative Procedure

Related Ministry Documents

N/A