Dufferin-Peel Catholic District School Board

DUFFERIN-PEEL CATHOLIC DISTRICT SCHOOL BOARD POLICY	
POLICY NUMBER:	P-5005
SUBJECT:	Cyber Security
REFERENCE:	P-5004: Acceptable Network Use and Security GAP5017: Cyber Security
EFFECTIVE DATE:	October 25, 2022
AMENDED DATE:	October 25, 2022

"The Lord is my rock, my fortress, and my deliverer; my God is my rock, in whom I take refuge, my shield and the horn of my salvation, my stronghold."
Psalm 18:2

1. Dufferin Peel Catholic District School Board (DPCDSB) recognizes digital information, information systems, education technology and internet connectivity as integral parts of DPCDSB's K-12 education system. They are essential in day-to-day operations, administrative functions, facilities management, and they help to enhance teaching and learning in school and during remote learning. As such, DPCDSB aims to take appropriate action to manage cyber risks and mitigate current and evolving cyber threats to: personal and sensitive information; DPCDSB information systems, network, and devices; educational technology and tools; internet-equipped DPCDSB facilities and equipment; and students and staff while online and using DPCDSB technology.

2. DPCDSB recognizes its responsibility in the stewardship of information technology, digital resources, security for personal information (PI), and other DPCDSB sensitive information that is stored on DPCDSB information systems. These may be on computers / servers located in DPCDSB buildings or in the cloud, within cloud service provider environments which may be distributed in multiple hosting facilities across different jurisdictions.

3. DPCDSB aims to facilitate secure, safe, responsible, and respectful use of technology to support teaching and learning and prepare students for the risks and opportunities of the digital world, to thrive safely online, and become good digital citizens. Key to meeting this objective is the implementation of three core areas of cyber protection: (1) cyber security to protect information technology (IT) and secure network-connected operational technology (OT) resources; (2) cyber/online safety to promote safe online practices and mitigate risks of inappropriate use of technology; and (3) online/digital privacy to protect personal information (PI) and other DPCDSB sensitive information from unauthorized access.

4. DPCDSB's comprehensive approach to cyber protection is described in this policy and in its associated *General Administrative Procedure (GAP) GAP5017: Cyber Security*, which forms an integral part thereof. This approach includes: cyber protection governance; cyber protection strategy/roadmap; cyber protection tools, standards, procedures, and guidelines; cyber protection assurance; and monitoring.

5. This policy and its associated GAP apply to: all DPCDSB departments, schools, staff, volunteers, and students who use DPCDSB information and IT resources; and all DPCDSB visitors (including parents and guardians), vendors, contractors, and other third-party individuals and organizations who have been authorized by DPCDSB to access DPCDSB IT resources and/or network resources, as applicable.

6. DPCDSB Information Security and Management System supports a cyber security strategy which seeks to mitigate risk and protect DPCDSB critical information against increasingly aggressive and sophisticated cyber threats while continually adapting to DPCDSB rapidly evolving needs.

7. As an integral component of this policy, *GAP5017: Cyber Security* enumerates the governance for cyber protection within DPCDSB to ensure everyone understands their roles and responsibilities.

8. DPCDSB shall implement a cyber security framework. The key platforms of the framework are information management, cyber security risk management, and cyber security incident management.

9. DPCDSB's cyber protection measures shall address: cyber security risk management, cyber risks associated with vendor supply chains and third party service providers, reliability and continuity of service, incident and breach response plans and management procedures, monitoring and audit processes, vulnerability and patch management, access control and authorization, and cyber awareness training.

10. DPCDSB's cyber protection measures shall comply with all applicable laws, legislation, and Ministry of Education policy directives.

11. DPCDSB shall ensure privacy and data protection. All individuals with access to PI and other DPCDSB sensitive information shall be required to comply with applicable DPCDSB policies, standards, procedures, and guidelines, and abide by all applicable privacy laws and legislations.

12. Legislation applicable to this policy and its associated GAP includes:

    a) *Education Act* - is the main law under which school boards operate. It contains board responsibilities for the effective stewardship of resources (including technology and data), promotion of student well-being, prevention of cyberbullying and protection of privacy.

    b) *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* - sets out the rules that school boards must follow regarding the collection, use, retention, and disclosure of personal information.

    c) *Personal Heal Information Protection Act (PHIPA)* – sets out the rules for collection, use and disclosure of personal health information by health information custodians, and it applies when students receive health care in school.