Dufferin-Peel Catholic District School Board

DUFFERIN-PEEL CATHOLIC DISTRICT SCHOOL BOARD BOARD POLICY	
POLICY NUMBER	P-5012
SUBJECT	Electronic Monitoring
REFERENCE	P-5005 Cyber Security GAP5017 – Cyber Security
EFFECTIVE DATE	October 25, 2022
REVIEWED/AMENDED	October 25, 2022

"Keep alert, stand firm in your faith, be courageous, be strong."
1 Corinthians 16:13

1 Dufferin Peel Catholic District School Board (DPCDSB) recognizes that electronic monitoring of all network traffic over the DPCDSB information communication technology infrastructure is a necessary component of DPCDSB's cyber security framework and the management of its assets.

2 DPCDSB engages in electronic monitoring of email, internet, and various hardware and software applications traversing its network infrastructure, including but not limited to: all DPCDSB computing devices; personal electronic devices (PEDs) connected to the DPCDSB network; physical security, building infrastructure, and life-safety systems; and global positioning system (GPS) enabled assets (i.e., vehicle telematics).

3 DPCDSB does **not** engage in the **active** electronic monitoring of staff and students. However, electronic monitoring of all network traffic traversing the DPCDSB infrastructure has the potential for investigation and/or electronic monitoring of staff and student activity.

4 DPCDSB may permit the inspection, monitoring, or disclosure of devices and systems connected to the DPCSDB network infrastructure in one or more of the following circumstances:

a) Inspection, monitoring, or disclosure is required by or consistent with applicable law, DPCDSB policies/procedures, or any appropriately issued subpoena or court order;

b) There is a reasonable suspicion that violations of law or DPCDSB policies/procedures have occurred or may occur;

c) There is a reasonable suspicion that a threat or threats to DPCDSB students, staff, and/or property have occurred or may occur;

d) There are time-dependent, critical operational needs of DPCDSB business, including response to allegations of misconduct by students or staff.

5 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 Health Information Protection Act (PHIPA)* – sets out the rules for collection, use and disclosure of health information, and it applies when students receive health care in school.

d) *Personal Information Protection and Electronic Documents Act (PIPEDA)* – sets out the rules that schools must follow regarding the collection, uses, or disclosures of personal information during commercial activities

e) *Employment Standards Act (ESA)* – within the context of this policy and as of January 1, 2022, the *ESA* requires organizations with 25 or more employees to maintain a written policy regarding the electronic monitoring of employees.