Hamilton-Wentworth Catholic District School Board
Believing, Achieving, Serving

Policy Manual – Information & Communication Technology

I.T.03 – Electronic Monitoring Policy

The mission of Catholic Education in Hamilton-Wentworth, in union with our Bishop, is to enable all learners to realize the fullness of humanity of which Our Lord Jesus Christ is the mode

POLICY STATEMENT

The Hamilton-Wentworth Catholic District School Board (Board) reserves its right to inspect, log, retrieve and archive data stored on Board-issued devices, and data transmitted across its network and communication technologies. The Board reserves the right to monitor communication and data at any time, with or without notice, to ensure that internet and communication technologies are being used only for Board business.

- No active monitoring or disclosure will occur without the direction of Senior Administration;
- Authorized Board Information Communication Technology (ICT) Services personnel may inadvertently view or access data files or messages while performing system maintenance or management functions. When this occurs, staff are required to keep the contents confidential. However, any suspected violations of law or Board policy will be reported to the Chief Information Officer (CIO).

Purpose

The Board, as the employer, retains ownership of the entire computer and network systems, including hardware, software, computer system files, documents and electronic communications. The Board's communication technologies are not intended for personal use by employees; therefore, their use and content may be monitored. E-mail, internet, or voice-mail communications are not private or personal despite any such designation by the sender or the recipient. Personal or private communications transmitted on the Board's electronic information system may be accessed, reviewed, copied, deleted, retained, or disclosed by the Board at any time and without notice.

The right of the Board to access an employee's internet history, documents and/or voicemail on Board provided technology, or when authenticated with HWCDSB user accounts on personal devices, may arise in a number of situations, including but not limited to:

- to comply with disclosure requests or orders made pursuant to the MFIPPA;
- for Board owned technology, because of regular or special maintenance of the electronic information systems;
- for Board owned technology, when the Board has a business-related need to access the employee's system, including, for example, when the employee is absent from work or otherwise unavailable;
- in order to comply with obligations to disclose relevant information in the course of a legal proceeding; and,
- and when the Board has reason to believe that there has been a violation of policy, or is undertaking an administrative, legal or disciplinary investigation.

Appendix A details routine electronic monitoring activities, mechanisms and purposes. The Board reserves the right to use any other monitoring activity at its discretion at any time as is reasonable in the circumstances in the event of an investigation of a safety, legal, administrative or disciplinary nature.

Responsibility
Superintendent of Human Resources
Chief Information Officer
Director of Education

Regulations
Employment Standards Act, 2000
ISO/IEC 27001: A.8.2 – Information Classification
Freedom of Information and Protection of Privacy Act (FIPPA, 2012)
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA, 2007)

Related Policies
A.11 Internet and Technology – Acceptable Use for Employees
A.12 Personal Mobile Devices (PMDs)
A.17 Privacy Breach
B.P.04 Key Control/Access to Buildings
H.M.04 Security Confidentiality and Protection of Personal Information
I.T.01 Information Classification Policy
I.T.02 Back-up and Restore Policy
S.15 Internet and Technology – Acceptable Use for Students

Related Board Committee
Committee of the Whole

Policy Review Date
BM Original Policy Approved 04 October 2022
Revisions:
To be reviewed every three years

Appendix A

Tool	Circumstances	How	Purpose
Network Monitoring	All internal and internet traffic when authenticated with HWCDSB user accounts on premise or roaming	Firewalls, Secure Access Service Edge tool and Security Information Event Management tool	To monitor for malicious traffic and indicators of compromise from malware.
Web filtering	All internet traffic when authenticated with HWCDSB user accounts on premise or roaming	Firewalls and Secure Access Service Edge tool	Protect from harmful and inappropriate content
E-Mail filtering	All e-mail traffic when authenticated with HWCDSB user accounts on premise or roaming	Data Loss Prevention	Prevent the transmission of private/confidential data over insecure e-mail
Account Authentication	Staff login to HWCDSB services on premise or roaming	Active Directory	To protect against unauthorized access
Device Management	Installed on all Board devices	Mobile Device Management	Protect against loss/ theft, and enforce security settings
Video surveillance (external and public areas only)	All buildings	Video surveillance cameras and recording systems	Safety, theft, illegal activity, behavioural/ incident monitoring and review.
Door Fobs	All buildings	Through door fob system	Control and monitor access to buildings.
Photocopiers/Printers	Board owned devices	Management console	Login audits and activity.
Global Positioning Systems (GPS)	Board owned vehicles	GPS Software	Detect and report on vehicle location of all vehicles during on-shift use.