Northeastern Catholic District School Board

ELECTRONIC MONITORING

Administrative Procedure Number: API003

POLICY STATEMENT

The Northeastern Catholic District School Board (NCDSB) is committed to protecting information privacy, safeguarding data systems, and maintaining secure and responsible use of its information and communication technology (ICT) resources.

In keeping with its commitment to transparency and accountability, the Board electronically monitors the use of its ICT systems in accordance with applicable legislation.

This policy governs the Board's authority to access and monitor data on its ICT systems and outlines the circumstances under which electronic monitoring of employees may occur, as required by Part XI.1 of the *Employment Standards Act, 2000*.

REFERENCES

Education Act
Employment Standards Act
Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
Effective Use of Technology (Ontario College of Teachers)
NCDSB Policy
- E-24 Personal Information Management
- I-1 Video Surveillance
- I-2 Responsible Use of Information and Communication Technology
- I-3 Electronic Monitoring

NCDSB Administrative Procedure
- APE024-1 Personal Information Management
- API002 Responsible Use of Information and Communication Technology

DEFINITIONS

Information and Communication Technology (ICT)
Includes use of hardware networks (computers, mobile devices, telephony, etc.) and related equipment as well as the use of information systems and applications such as computer software, electronic mail, web pages, cloud-based applications and the internet, whether used within the Board or in a way that has a connection to the Board.

Personal Network Device
A device, owned by a User, which has the capability to connect to a computer network, either through a network wire or using a radio designed to connect to a wireless computer network. Examples include: laptops, net books, portable game devices, and cellular telephones.

Users
Any person (employee, student, trustee, visitor) who uses the NCDSB ICT systems and services.

PROCEDURES

1.0 GENERAL PROVISIONS

1.1 This administrative procedure applies to all NCDSB ICT systems, including employees, students, trustees, contractors, volunteers, and any other individuals granted access to Board-owned or Board-managed systems, networks, devices, or facilities.

1.2 Electronic monitoring shall:

i) be conducted for legitimate and lawful purposes;
ii) be reasonable, proportionate, and limited to what is necessary;
iii) respect personal privacy to the greatest extent possible;
iv) be carried out in a transparent manner;
v) comply with the *Education Act*, *Employment Standards Act, 2000*, the *Municipal Freedom of Information and Protection of Privacy Act*, and other applicable legislation.

1.3 Electronic monitoring is primarily automated and event-driven, with information typically reviewed in response to system alerts, flags, or notifications, or where otherwise reasonably required for legitimate purposes.

1.4 This administrative procedure will be reviewed periodically to ensure ongoing compliance with legislation and alignment with Board policies.

2.0 LEGITIMATE PURPOSES FOR MONITORING

2.1 The NCDSB may access and monitor ICT system for purposes that include but are not limited to:

i) maintaining the security, integrity, and functionality of ICT systems;
ii) protecting students, staff, and Board property;
iii) detecting, preventing, or investigating misuse, security incidents, or breaches of Board policies;
iv) ensuring compliance with Board policies, procedures, and standards;
v) supporting operational continuity, system maintenance, and planning;
vi) fulfilling legal, regulatory, or audit requirements.

3.0 TYPES OF ELECTRONIC MONITORING

3.1 Network Monitoring

The Board uses tools to filter, log, and analyze network traffic entering and leaving ICT networks. Network monitoring may collect information such as:

i) user identifiers;
ii) source and destination of network communications;
iii) type of application or service used;
iv) date and time of activity;
v) indicators of potential security threats or anomalous behaviour.

3.2 Application and System Monitoring

Applications and systems used or managed by the Board (email, phone, financial, learning management, student information system)

i) user access and authentication events;
ii) dates and times of use;
iii) system actions performed by users;
iv) limited location data, where supported by the system.

3.3 Device Monitoring

The Board uses device management and security tools to monitor Board-owned devices and personal devices when connected to Board networks or accessed using Board credentials. This may include:

i) malware and security threat detection;
ii) device compliance and configuration status;
iii) connection location and device identifiers;
iv) indicators of unauthorized use.

3.4 Video Surveillance Monitoring

Video surveillance systems are used in Board facilities to support the safety and security of students, staff, visitors, and property. Video surveillance is governed by the Board Video Surveillance policy and attendant administrative procedures.

3.5 Access Control Monitoring

Electronic access control system (cards) record:

i) user identity;
ii) point of entry;
iii) date and time of access.

In select areas, electronic systems may also be used to record employee sign-in and sign-out times for payroll and operational purposes.

3.6 Performance Monitoring

Where applicable, electronic systems may be used to track and measure specific employee tasks against pre-established benchmarks. Information collected may be used for:

i) operational planning;
ii) service improvement;
iii) workforce and resource management;
iv) performance management in accordance with applicable policies.

4.0 ENHANCED OR INVESTIGATIVE MONITORING

4.1 The Board may employ enhanced monitoring tools or adjust existing monitoring settings where reasonably necessary to:
i) investigate suspected misconduct or policy violations;
ii) respond to security incidents or emerging threats;
iii) comply with legal obligations.

4.2 Enhanced monitoring shall be authorized by the Chief Executive Officer and conducted in a manner that is reasonable and proportionate.

5.0 USE, ACCESS, AND DISCLOSURE OF INFORMATION

5.1 Information collected through electronic monitoring shall be:
i) accessed only by authorized personnel;
ii) used solely for legitimate Board purposes;
iii) protected through appropriate administrative, technical, and physical safeguards.

5.2 Information may be disclosed where required or permitted by law, including for legal proceedings, audits, or regulatory compliance.

6.0 RETENTION AND DISPOSAL

6.1 Information collected through electronic monitoring shall be retained and disposed of in accordance with:
i) the Board's records retention schedule;
ii) applicable privacy legislation;
iii) operational and legal requirements.

7.0 ROLES AND RESPONSIBILITIES

7.1 Chief Executive Officer
i) Ensuring electronic monitoring practices comply with legislation and Board policy.
ii) Approving enhanced monitoring activities.
iii) Ensuring transparency and accountability.

7.2 Information and Communication Technology Services
i) Implementing and maintaining monitoring tools.
ii) Safeguarding monitored information.
iii) Supporting investigations and audits as authorized.

7.3 Supervisors and Managers

i) Ensuring staff are aware of this policy and administrative procedures.
ii) Using monitoring information appropriately and lawfully.
iii) Consulting Human Resources where monitoring relates to employee conduct or performance.

7.4 Users

i) Using ICT systems in accordance with Board policies and administrative procedures.
ii) Understanding that there is no expectation for privacy when using Board ICT systems.

8.0 RELATED FORMS AND DOCUMENTS

Nil.

Chief Executive Officer: *Tricia Stefanic Weltz*
Date: March 2026