Northeastern Catholic District School Board

ELECTRONIC MONITORING	
Policy Number: I-3	**Authority: 23-18**

POLICY STATEMENT

The Northeastern Catholic District School Board (NCDSB) is committed to ensuring information privacy and security for its staff and data systems. The NCDSB also wishes to be transparent in its data security and electronic monitoring policies.

This policy governs the NCDSB's access to data on its ICT network. It also discloses how and under what circumstances the NCDSB may electronically monitor employees 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

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.

POLICY REGULATIONS

1.0 ICT ACCESS

1.1 The NCDSB provides the ICT systems to Users to enable productive work. The NCDSB may access accounts and information for its legitimate purposes, which include:

i) performing ICT maintenance and repair;
ii) investigating ICT misuse;
iii) upholding NCDSB security and safety;
iv) auditing compliance with NCDSB policies;
v) complying with a legal or regulatory obligations, including as required under the *Education Act* and the *Municipal Freedom of Information and Protection of Privacy Act*;
vi) supporting work and work continuity on ICT systems;
vii) conducting research to support NCDSB planning; and
viii) any other purposes as permitted by law.

1.2 Personal use of ICT devices and systems is a privilege. Users should have no expectation of privacy given these purposes. If Users need privacy, they should use a personal device that is not connected to the NCDSB network or other ICT systems. A password allows the NCDSB to identify how you are using ICT resources, and does not preclude the NCDSB from accessing data on ICT resources.

2.0 ELECTRONIC MONITORING

2.1 The NCDSB electronically monitors Users, including employees, for the legitimate purposes listed above.

2.2 The NCDSB routinely collects the following information and accesses it on an as-needed basis. The NCDSB reserves the right to employ special monitoring tools or change settings and parameters of existing monitoring tools as part of a reasonable investigation, to address a changing threat environment or for other operation needs.

i) Network Monitoring
Tools for filtering and logging traffic in and out of the ICT networks.

Network monitoring provides data on who is communicating in and out of the ICT networks, what type of application they are using to communicate, when they are using it, and whether the traffic may indicate a security problem.

ii) Application Monitoring
Tools for managing how applications and systems are used.

Applications and systems (phone systems, email system, financial system, teaching systems, etc) monitoring typically provides data on who has used an application and when.

Applications and systems may also track User actions and locations though this varies depending on the application or system.

iii) Device Monitoring
Tools for managing and detecting anomalous events on various devices (NCDSB owned devices, Personal Network Devices connected to the ICT networks and/or remotely connected to the ICT networks using NCDSB's account credentials).

Device monitoring (anti-malware software, anti-virus software, device management software and configuration tools) provides data to determine if a device is being used without authorization or if there is another problem on a device.

Device monitoring may also track the location from which a device connects, and information on Personal Network Devices when connected to ICT networks.

iv) Video Surveillance Monitoring
Tools for monitoring physical activity on the NCDSB premises.

The NCDSB employs video surveillance across its facilities for the purpose of supporting the safety and security of students, staff, and property.

v) Access Control Monitoring
Tools for managing access to NCDSB facilities.

The NCDSB employs electronic systems for controlling access to its facilities. If an NCDSB facility is accessed using a NCDSB access cards/fobs, these systems will record the User identity, the point of entry and the time and date of entry.

In select areas, departments may additionally utilize systems to track employee shift sign-in and sign-out times to support payroll activities.

vi) Performance Monitoring
Tools for benchmarking employee performance.

The NCDSB employs electronic systems for tracking and measuring certain employee tasks against pre-defined benchmarks. This information is used to monitor employee performance and may be used in personnel planning and for operational decision-making.