St. Clair Catholic
District School Board

Policy & Procedures
PROCEDURE
Sec. D: Staff and Volunteers

Electronic Monitoring

Date: 2023 03 28

Administrative Procedures

This Administrative Procedure outlines the forms of electronic monitoring in use by the Board, for the purpose of ensuring a safe working environment for staff and students and the continued safety and efficiency of the Board's operations. The purpose of this procedure is to provide a description of how and in what circumstances the Board electronically monitors employees and the purpose for which the information obtained through electronic monitoring may be used. A list of electronic systems that may be monitored is provided in Appendix A.

1. Responsibilities

1.1 The Director of Education is responsible for ensuring the implementation of and compliance with this Administrative Procedure, including the designation of required resources.

1.2 Human Resource Services is responsible for ensuring all new employees receive a copy of this Administrative Procedure and ensuring current employees are required to review annually.

1.3 Superintendents, Principals, Vice Principals, Managers, and Supervisors are responsible for having an understanding of this Administrative Procedure and ensuring all monitoring is aligned with this Administrative Procedure.

1.4 All Staff are responsible for having an understanding of this Administrative Procedure and reviewing this Administrative Procedure annually.

2. Expectations of Electronic Monitoring

2.1 The Board conducts electronic monitoring for the following reasons and in the following circumstances.

a. The Board conducts electronic monitoring to ensure we:

i. Protect staff, students, and technology from harm
ii. Keep our facilities and property safe and secure
iii. Protect electronic resources from unauthorized access
iv. Protect against loss, theft, or vandalism

b. Routine Monitoring: The Board routinely monitors electronic systems. The Board may monitor and access any files, documents, electronic communications, and use of the internet at any time to ensure the integrity of our electronic systems.

c. Demand Monitoring: The right of the Board to access data collected via our electronic systems (Board provided technology or personal devices when using Board credentials and/or networks) may arise in a number of situations, including but not limited to:

i. To comply with legislative disclosure or access requirements under MFIPPA (Municipal Freedom of Information and Protection of Privacy Act) and PHIPA (Personal Health Information Protection Act) or to assist with the investigation and resolution of a Privacy Breach.
ii. For Board owned technology, because of regular or special maintenance of the electronic information systems.
iii. 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.
iv. In order to comply with obligations to disclose relevant information in the course of a legal matter or legislated requirement.
v. When the Board has reason to believe that there has been a violation of the Code of Conduct, Board Policy, or is undertaking an administrative, legal, or disciplinary investigation.
vi. For Video Surveillance, as outlined in the Board's Video Surveillance Policy and Procedure.

2.2 The Board may, in its discretion, use information obtained through electronic monitoring to determine if there has been a violation of its policies and/or any other misconduct. Where appropriate, such information may lead to disciplinary action, up to and including termination of employment.

2.3 This Policy and Procedure seeks to meet the requirements put in place by recent legislative amendments. Nothing in this Policy shall be interpreted to create any greater right or benefit than what is available under existing legislation, or to restrict any of the Board's legal rights.

3. Additional Information

3.1 The St. Clair Catholic District School Board is committed to the principles of equity and inclusive education, consistent with our Catholic teachings, which value and promote human rights and social justice in all Board policies, programs, guidelines, operations and practices.

Definitions

- **Demand Monitoring**: Electronic monitoring in which critical business systems and/or logs for those systems are accessed due to a legitimate business requirement.

- **Electronic Monitoring**: Review of the data or output of electronic systems deployed on corporate networks, devices, as well as work tools with embedded sensors (e.g., telematics and similar technologies).

- **Electronic System**: A device connected via wired or wireless communication to exchange real time data. This includes end user devices but also the servers and systems the Board uses to conduct their business. Examples include email, firewalls, ventilation controls and wireless access points.

- **Personal Network Device**: An end user device, owned by the 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, netbooks, some portable music players, some portable game devices and most cellular telephones.

- **Routine Monitoring**: Electronic monitoring in which critical business systems are routinely checked against quality control rules to make sure they are always of high quality and meet established standards.

References

- Bill 88, Working for Workers Act (Amendment), 2022
- Employment Standards Act, 2000
- Responsible Use of Technology Policy and Procedure
- Video Surveillance Policy and Procedure
- Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56
- Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched.

Appendix A – Electronic Monitoring Applicable Systems

Tool	What is monitored?	How	Purpose
Vehicle telematics / GPS	All fleet vehicles during use	Vehicle sensors	To allow information about fleet management, driver safety and theft
Network Monitoring	All network traffic	Packet analysis/log collection	To ensure service management and network protection is maintained
Web-Filtering	All internet traffic	Firewall system	To protect from harmful or inappropriate online content
Account Authentication	Staff login to services	Authentication Server	Protection against unauthorized access
VPN	Staff remote login to services	Authentication Server and application	Protection against unauthorized access
Electronic Communications	All e-mail traffic	Exchange/Gmail system	Prevent the transmission of inappropriate/confidential data over unsecure e-mail.
Access Cards (FOB)	Each scan at door readers	Door access control system	Control access to buildings and shared printers at all facilities. Also used to lock-down facilities in an emergency situation.
Device Management (laptop/desktop)	Installed on all Board laptops/desktops.	Mobile device management console	Protects against loss/theft and enforces security settings to ensure cyber protection and safe use.
Device Management (Chromebooks)	Installed on all Board Chromebooks.	Management console	Protects against loss/theft and enforces security settings to ensure cyber protection and safe use.
Device Management (iPADs)	Install on all Board iPads	Management console	Protects against loss/theft and enforces security settings to ensure cyber protection and safe use.
Device Management (Board Cell Phones)	Installed on all Board managed cell phones	Management console	Protects against loss/theft and enforces security settings to ensure cyber protection and safe use.
Video Camera Systems	Some facilities, exterior and internal hallways	Video surveillance cameras and recording systems	Protects against loss/theft, illegal activity, behavioral/incidents. Monitors and detect any suspicious activity in a designated area inside or outside of a school or facility.
Board supported applications	Staff login and data changes	Authentication Server and/or built into specific application	Protection against unauthorized access and history of data changes.
Phone System	All facilities	Private Branch Exchange (PBX) phone system	To ensure service management such as call quality (bandwidth, latency, jitter, packet loss, compression), call volume and voicemail storage monitoring.