CATHOLIC DISTRICT
SCHOOL BOARD OF
EASTERN ONTARIO
www.cdsbeo.on.ca

BOARD ADMINISTRATIVE PROCEDURE

ADMINISTRATIVE PROCEDURE

601 Electronic Monitoring

DIRECTIONAL POLICY

Nurturing Human Resources

Title of Administrative Procedure:

Electronic Monitoring

Date Approved:

October 2022

Projected Review Date:

October 2027

Directional Policy Alignment:

This Administrative Procedure aligns with the Nurturing Human Resources Directional Policy - #600. CDSBEO is committed to the continued safety and efficiency of its operations and ensuring a safe environment for the work of our students and staff. The purpose of this Administrative Procedure is to outline the electronic monitoring in use by the Board to meet that commitment.

Alignment with Multi-Year Strategic Plan:

This policy aligns with the Multi-Year Strategic Plan objective of **Protecting**. Specifically, the Priorities of:

- Foster safe learning environments that ensure the mental and physical health of our students as a priority.
- Set priorities for the use of fiscal resources which are consistent with the Board's Vision and Mission statements, and comply with the Ministry of Education's mandates, regulations, and guidelines.

This Administrative Procedure supports safe learning by leveraging electronic monitoring to ensure the safe and effective use/occupancy of Board resources and facilities.

CDSBEO Strategic Plan 2020-2025

Action Required

Employers of over 25 employees in Ontario are required to have a written policy in place with respect to electronic monitoring of employees. CDSBEO routinely monitors our electronic systems. A list of systems is provided in Appendix A.

Scope:

This Policy applies to all employees of the Board.

Electronic Monitoring Conducted by the Board and Purposes for Which Electronic Monitoring May be Used:

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

1. The Board conducts electronic monitoring to ensure we:
    a. Protect staff, students, and technology from harm
    b. Keep our facilities and property safe and secure
    c. Protect electronic resources from unauthorized access
    d. Protect against loss, theft, or vandalism
2. 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.
3. 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 several situations, including but not limited to (approvals required indicated in parentheses):
    a. 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. (Requested by Manager of Communications and approved by the Director of Education).
    b. For Board owned technology, because of regular or special maintenance of the electronic information systems (Requested by authorized ICT Staff and Approved by Manager of Information Technology).
    c. 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 (Requested by Supervisor and Approved by the Manager of Information Technology).
    d. In order to comply with obligations to disclose relevant information in the course of a legal matter (Requested by the Human Resource Services Manager or Supervisory Officer and approved by the Director of Education or Superintendent of Business).

e. 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 (Requested by Authorized Human Resource Services staff and Approved by a member of Senior Administration.)
f. For Video Surveillance, as outlined in D1:7 - Video Surveillance

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.

No Greater Right or Benefit:

This Policy 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.

Responsibilities

The Board of Trustees is responsible for:

- Ensuring alignment with the Human Resources Directional Policy.
- Reviewing the Electronic Monitoring Administrative Procedure as part of its regular policy and procedures review cycle and as required by legislation.

The Director of Education is responsible for:

- Ensuring the implementation of and compliance with this Administrative Procedure, including the designation of required resources.

Superintendents of Schools and System Portfolios are responsible for:

- Understanding this Administrative Procedure.
- Ensuring all monitoring is aligned with this Administrative Procedure.

Principals and Vice-Principals are responsible for:

- Understanding this Administrative Procedure.
- Ensuring all monitoring is aligned with this Administrative Procedure.

Staff are responsible for:

- Understanding this Administrative Procedure.
- Reviewing this Administrative Procedure annually.

Progress Indicators

- Awareness of the policy by all staff in the Board.

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

- Working for Workers Act, 2022, S.O. 2022, c. 7 – Bill 88
- Employment Standards Act, 2000 , S.O. 2000, c. 41
- Administrative Procedure 801 Employee Acceptable Use of Technology Procedure
- Administrative Procedure F1:6 – ICT Security Procedure
- Administrative Procedure F3:1 – Information and Records Management
- Administrative Procedure D1:7 - Video Surveillance
- 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. A

Appendix ‘A’:

Tool	What is Monitored?	How	Purpose
Web filtering	All internet traffic	Firewalls and or End Point Protection	Protect from harmful and inappropriate content.
Electronic communications filtering	All electronic communications traffic	Safety and Security	Prevent the transmission of inappropriate/confidential data over insecure electronic communications. Maintain the integrity of the data.
Network Monitoring	All network traffic	Packet analysis	Protect the integrity and availability of the network.
Account Authentication	Staff login to services	Authentication Server	Protect against unauthorized access.
Device Management	Installed applications	Device Management and Endpoint Security	Protect against loss/ theft and enforce security settings.
Phone logs	Some facilities, incoming and outgoing phone logs	Private Branch Exchange (PBX) phone system and/or VoIP Phone System	Call quality (e.g., bandwidth, latency, jitter, packet loss, compression), call volume and voicemail storage monitoring
Video surveillance	Some facilities, entries, building exterior and internal hallways.	Video surveillance cameras and recording systems	Safety, theft, illegal activity, behavioural/incident monitoring, and review.
Access Cards	Some facilities, building entry events	Through Door Reader	Control and monitor access to buildings.
Electronic sign-in	Log of individuals entering and exiting the building	Electronic data collection	Maintaining a Visitor’s Book per the Education Act and where necessary for health-related purposes.
Vehicle Tracking	Vehicle Location	Vehicle location GPS Trackers	Ensure the proper utilization of Board owned vehicles.