Waterloo Catholic District School Board
Quality, Inclusive, Faith Based Education

Administrative Procedures Memorandum APS051

Electronic Monitoring

Date of Issue: October 17, 2022
Reviewed/Revised: October 17, 2022

Memo To: All Staff

From: Director of Education

ACCESSIBILITY:

To request this file in large print, please email aoda@wcdsb.ca or call (519) 578-3660.

PURPOSE:

Employers of over 25 employees in Ontario are required to have a written policy in place with respect to electronic monitoring of employees. The Waterloo Catholic District School Board (WCDSB) routinely monitors our electronic systems. A list of systems is provided in Appendix A.

REFERENCES:

- Employment Standards Act Requirement, Bill 88: Electronic Monitoring Policy, Written policy on electronic monitoring of employees | Your guide to the Employment Standards Act | ontario.ca
- Bill 88, Working for Workers Act (Amendment), 2022
- Employment Standards Act, 2000
- Responsible Use of Information Technology and Electronic Data – Staff – APS017
- Records Information Management – APC016
- Video Surveillance – APC028
- 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

FORMS:

- N/A.

REPORTS:

- N/A.

APPENDICES:

- Appendix A: Electronic Monitoring - Applicable Systems

COMMENTS AND GUIDELINES:

Electronic Monitoring Conducted by the Board:

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

1. The Board conducts electronic monitoring to ensure we:

   - Protect staff, students and technology from harm.
   - Keep our facilities and property safe and secure.
   - Protect electronic resources from unauthorized access.
   - 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 a number of situations, including but not limited to (approvals required indicated in parentheses):

   a. To comply with legislative disclosure or access requirements under Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and Personal Health Information Protection Act (PHIPA) or to assist with the investigation and resolution of a Privacy Breach (Requested by Privacy Officer and approved by the Director of Education, or, as part of delegated responsibilities under MFIPPA).

   b. For Board-owned technology, because of regular or special maintenance of the electronic information systems (Requested by authorized IT Staff and Approved by the Chief Information Officer).

   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 Chief Information Officer).

   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 Video Surveillance – APC028

Purposes for Which Electronic Monitoring May Be Used:

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

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 Employee Relations 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.

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.

Superintendents, Principals, Vice Principals, Managers, and Supervisors are responsible for:

- Having an understanding of this Administrative Procedure.
- Ensuring all monitoring is aligned with this Administrative Procedure.

All Staff are responsible for:

- Having an understanding of this Administrative Procedure.
- Reviewing this Administrative Procedure annually.

Definitions:

- Board owned technology includes devices such as computers or phones, and also includes information assets or user accounts provisioned and managed by the Board.
- 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.