Algonquin & Lakeshore
Catholic District School Board

ADMINISTRATIVE PROCEDURES

Electronic Monitoring (Policy Statement: Electronic Monitoring)

Purpose

This 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.

References

Bill 88, *Working for Workers Act* 2022
Employee Standards Act, 2000
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
Policy A-2017-11-1 - Freedom of Information and Protection of Privacy Policy
Policy A-2019-05-8 - Digital Citizenship Policy
Policy S-2013-05-04 Caring and Safe Schools
Applicable Collective Agreements and Terms of Employment

1. Definitions:

1.1 Demand Monitoring

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

1.2 Electronic Monitoring

The review of data or output of electronic systems deployed on board networks, devices, as well as work tools with embedded sensors (e.g., telematics and similar technologies).

1.3 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.

1.4 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.

1.5 Personal Network Device

A 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.

Procedures

2. Scope

The application of this Policy and Administrative Procedure includes:

2.1 the use of all Board-owned technology, such as computers, mobile devices, and networks regardless of where they are used. This includes the use of Board-owned technology when used off Board property.

2.2 the use of personally owned technology, including personally owned computers and mobile devices, when used to access the Board network and applications.

2.3 any access to Board technology resources regardless of the location and ownership of the devices used to access Board resources. This includes remote working, wireless access to the Board network, websites, and applications.

3. Electronic Monitoring Conducted by the Board:

The Board conducts electronic monitoring for the following reasons and in the following circumstances as outlined in Appendix 1- Electronic Monitoring. Electronic Monitoring is done to ensure:

a) The protection of staff, students, and technology from harm
b) The safety and security of Board facilities and property
c) The safeguarding of electronic systems and networks from unauthorized access
d) Protection against loss, theft or vandalism

3.1 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.

3.2 Demand Monitoring: The right of the Board to access data collected related to the operation of the Board via our electronic systems, as authorized by the Director of Education or designate (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:

3.2.1 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.

3.2.2 For Board owned technology, because of regular or special maintenance of the electronic information systems.

3.2.3 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.

3.2.4 In order to comply with obligations to disclose relevant information in the course of a legal matter or legislative requirement.

3.2.5 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.

3.2.6 For video surveillance of Board facilities and property

4 Purposes for Which Electronic Monitoring May Be Used:

The Board may, in its discretion, use information obtained through electronic monitoring if there is reason to believe 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.

5 No Greater Right or Benefit

This Policy seeks to meet the requirements put in place by 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.

The Board reserves the right to amend or revise this policy in accordance with operational requirements and any legislative changes.

Appendices
Appendix A- Electronic Monitoring Appendix

Forms

Associated Documents

Approved: October 2022