



Limestone District School Board is committed to the safe, efficient, and effective use of Board resources and facilities in its day-to-day operations. The purpose of this Administrative Procedure is to outline the Board's responsibilities and capabilities regarding electronic monitoring. Electronic monitoring will be implemented in a fair and transparent manner and only for the purposes for which it is established. The Board reserves the right to monitor employee usage of Board technology, systems and services, including monitoring email usage, internet usage, and access and use of Board technology systems. Personal or private communications transmitted on the Board's electronic information system may be accessed, reviewed, copied, deleted, retained, or disclosed by the Board at any time and without notice to the employee.

Application and Scope

This procedure applies to all employees, contractors, volunteers and trustees, whether working in the workplace, working remotely, or a combination thereof and describes how and in what circumstances the Board electronically monitors its employees, the mechanisms, and the purpose(s) for so doing. There is no absolute expectation of privacy in using Board owned technology. The Board monitors and accesses electronic communications, Internet history/traffic, files, documents, and the overall system, where deemed necessary, to ensure security. The monitoring mechanisms ensure the system's integrity and compliance with LDSB procedures.

All electronic communication and Internet communications sent and received by users while using their Board-issued credentials are the property of the Board. Communications are not private or personal despite any such designation by the sender or the recipient and personal or private communications transmitted on the Board's electronic information system (email platform) may be accessed, reviewed, copied, deleted, retained, or disclosed by the Board at any time and without notice to the employee.



Definitions

Electronic Monitoring means any form of monitoring of Board technology, systems, and services that is done electronically. Examples of electronic monitoring by the Board include:

- a. Using a Global Positioning System (GPS) to track the movement of a fleet vehicle operated by an employee
- b. Monitoring the websites that employees visit while accessing Board technology;
- c. Filtering of all web and email traffic;
- d. Device management;
- e. Controlling and monitoring access to buildings with Board access cards;
- f. Monitoring internet usage; and,
- g. Monitoring use and access of Board technology systems on a personal or corporate device.

For purposes of this procedure, electronic monitoring does not include photographic or video surveillance, which is covered under Administrative Procedure 194.

Principles

This Administrative Procedure is constructed to adhere to laws and regulations passed by the Province of Ontario and guidelines issued by the Ministry of Labour. Specifically, this procedure seeks to follow the Working for Workers Act 2021, along with any guidance provided by the Ministry of Labour, as amended from time to time.

Electronic Monitoring Conducted by the Board

From a risk management perspective, electronic monitoring serves to:



- Protect staff, students, and technology from harm
- Increase the safety and security of our facilities and property
- Protect electronic resources from unauthorized access
- Protect against loss, theft, or vandalism

Employee use of Board technology may be reviewed under a variety of circumstances, including, but not limited to:

- a) If there are reasonable grounds to suspect misconduct or improper use of Board technology, systems, or equipment;
- b) Complying with disclosure requests or orders made pursuant to complying with disclosure requests under MFIPPA (Municipal Freedom of Information and Protection of Privacy Act) or to assist with the investigation and resolution of a Privacy Breach;
- c) Regular or special maintenance of electronic information systems;
- d) Business related requirements to access Board owned, employee devices/technology. For example, when an employee is absent from work or otherwise unavailable;
- e) Complying with obligations to disclose relevant information in the course of a legal matter as requested by the Director of Education, Superintendent of Human Resources or Superintendent of Business; and,
- f) When the Board has reason to believe that there has been a breach of policy/procedure, or is undertaking an administrative, legal and/or disciplinary investigation.



Improper use of technology systems and services may be subject to disciplinary action, up to and including termination of employment.

Responsibilities

The Board is responsible for maintaining compliance with all statutory duties and obligations under the Employment Standards Act, as amended, and other relevant legislation.

The Superintendent of Human Resources and Associate Superintendent of Programs & Information Technology Services, or designates, are responsible for ensuring compliance with this procedure and approving requests to review employee usage of Board technology, systems or equipment.

Senior Management is responsible for submitting requests to review employee usage of Board technology, systems, or equipment to the Superintendent of Human Resources, or designate, and reviewing employee usage of Board technology, systems, or equipment if approved to do so.

Information Technology Services is responsible for receiving and processing requests to review employee usage of Board technology.

Employees are responsible for using Board technology, systems, or equipment appropriately in accordance with AP 146 – Digital Citizenship.



Legal References

Bill 88, Working for Workers Act

Education Act, as amended

Employment Standards Act, as amended

Administrative Procedure 146 – Digital Citizenship

Administrative Procedure 401 – Personnel Files & Collection of Personal Data

Administrative Procedure 444 – Use of Social Media



Examples of Monitoring in LDSB

Appendix A

Tool	What is monitored	How	Purpose
Web Filtering	All internet traffic	Firewalls	Protect from harmful and inappropriate content
E-Mail Filtering	All e-mail traffic	Data Loss Prevention	Prevent the transmission of inappropriate/confidential data over insecure e-mail
Network Monitoring (wifi/Internet)	All network traffic	Packet Analysis	Protect the integrity and availability of the network
Account Authentication	Staff login to services	Active Directory	Protect against unauthorized access
Device Management (iPad/iPhone)	Installed on all Board iPads/iPhones	Mobile Device Management	Protect against loss/ theft, and enforce security settings
Device Management (Chromebook)	Installed on all Board Chromebooks	Management Console	Protect against loss/ theft, and enforce security settings
Device Management (Laptop)	Installed on one-to-one/administrative laptops	Endpoint Security Tool	Protect against loss/ theft, and enforce security settings
Phone Logs	Some facilities	Phone system or PBX Logs	Call quality (e.g. bandwidth, latency, jitter, packet loss, compression), call volume and voicemail storage monitoring
Video surveillance	Some facilities	Video Surveillance Cameras and Recording Systems	Safety, theft, illegal activity, behavioural/ incident monitoring, and review.
Access Cards	All facilities	Through Door Reader	Control and monitor access to buildings.
Access Cards	All facilities	Photocopiers	Control and access to printing and photocopiers
GPS	In some Board-owned vehicles	GPS Tracking System and Associated Software	Protect against loss and theft. Staff safety in case of breakdown. Administrative investigations.