Policy on Electronic Monitoring

Office of Administration:	Vice-President Finance and Administration
Approval Authority:	Executive Team
Approval Date:	October 4th, 2022
Last Review:	Not applicable
Next Review:	August 2025

1. Purpose

1.1 This Policy on Electronic Monitoring (the “Policy”) is intended to:

1.1.2 State Laurentian University of Sudbury’s (the ”University”) commitment to clear, concise and transparent sharing of information related to the uses of, and reasons for, electronic monitoring of employees on the University infrastructure, information systems and end-user devices; and

1.1.3 Meet the requirements of Electronic Monitoring under the *Employment Standards Act, 2000* of Ontario as defined by Bill 88, *Working for Workers Act, 2022*.

2. Scope

2.1 This Policy applies to all Laurentian University (hereinafter referred to as “the Employer”) employees, in any capacity, as defined by the term “employee” under the *Employment Standards Act, 2000,* and shall hereinafter be referred to as Employee(s).

2.2 This Policy will not cover items that the Employer deems to be the normal course of business operations or in the course of performing its fiduciary duty to implement technical, financial and operational controls to monitor transactions or ensure compliance (e.g. monitoring of purchases on a corporate credit card).

3. Principles

3.1 Electronic Monitoring measures, are:

- In response to a legitimate academic or research need;
- Protecting an employee’s digital safety and data privacy;
- For quality control, quality assurance programs, continuous improvement and/or business analytics; and,

- Used for workforce and capacity planning

3.2 Definitions

"*University Campus(es)*" - means all University owned and operated spaces, including, but not limited to: offices, student residences, classrooms, labs, study spaces, libraries, recreational facilities, dining halls and eateries, buildings, building entrances, loading docks, University vehicles and outdoor areas.

"*Electronic Monitoring*" - the collection and/or use of information about an employee by an employer, for the benefit of an employer, by means of electronic equipment, software (including those managed or hosted by a third-party, e.g cloud software) or electronic network.

"*Employer*" - Laurentian University of Sudbury and all subsidiaries and affiliate groups subject to organizational policies, standards and procedures.

"*Employee*" - an individual who performs work, in any capacity, for an employer ("Laurentian University") as defined by the *Employment Standards Act* of Ontario. Without limiting the generality of the foregoing, this includes paid and unpaid employees, contractors, temporary assignment and digital workers, who work on campus, remotely or in a hybrid capacity.

"*Active Monitoring*" - the intentional tracking of activities and events, usually in real time, including without limitation: audit logs, audio and video files, camera footage, physical entry logs and location information, that are actively reviewed on a regular basis.

"*Passive Monitoring*" - The collection of data, activities and events, as a result of automated systems to maintain business operations. The collected data is used to troubleshoot, address a technical issue or to provide retrospective analysis. Passive monitoring may also encapsulate identifiable "presence" or availability information as can be seen in free/busy statuses in online calendars, chat or collaboration suites.

"*Record*" - means any record of information, however recorded, that contains identifiable information about an individual in relation to an activity or event.

4. Policy Statement

4.1 General

4.1.1 The employer will only actively electronically monitor its employees for reasons listed in section 4.2 and in congruence with the principles and uses of monitored data in section 3.

4.1.2 The employer shall use the recorded events and activities for the purpose for which it was obtained and communicated and where its purpose remains consistent.

4.1.3 The employer shall make every effort to inform the employee, using explicit statements and warnings, where technology permits, or using awareness and training, that an employee is being actively monitored prior to the employer engaging in monitoring activities.

4.1.4 Employees shall accept that employee-owned end-user devices may be monitored by the employer by virtue of their association with the University's infrastructure services. Any service, application and hardware that is connected to the University infrastructure by user credentials or unique and identifiable tokens may be monitored.

4.1.5 This policy does not supersede any rights an employee may have under a collective agreement or employment contract with the employer.

4.1.6 This policy does not provide new rights or privileges to employees to not be electronically monitored.

4.1.7 Information gathered by passive monitoring may include identifiable information about one or many parties and may be used or correlated against other datasets at the employer's discretion. Correlation of data will be done in accordance with university policies.

4.1.8 The employer may use data collected and retained from active and passive electronic monitoring for the purpose of evaluating or investigating employee performance, behaviour or conduct. The University may use the data for disciplinary purposes, up to and including termination of employment.

4.1.9 The employer may use data that has been collected and retained from active and passive electronic monitoring for the purpose of investigating physical security events and incidents, cybersecurity events, or when there is just cause of a suspected violation of university standards and policies and/or municipal, provincial, or federal laws. All investigations will be conducted in compliance with relevant statutes, legislation and University policies.

4.1.10 This Policy may be amended, by the University at its own discretion, at any time for any reason. Amendments to the policy will be shared with employees at least thirty (30) calendar days before the changes are in effect.

4.1.12 The employer shall retain a copy of this Policy and any subsequent versions for a period of three (3) years after it ceases to be in effect.

4.2 Types of Electronic Monitoring

4.2.1 The University will, in general terms, electronically monitor the following systems, events and activities:

Cameras & physical access			
Category	**Summary of monitoring activities**	**Type of monitoring**	**Type of record**
CCTV/ Security management	University campus cameras record video footage of various areas, (indoors and outdoors)	Passive	Video
Door access & digital badges	Entry and/or exits via an access card, smart card or other digital badging technologies are recorded by the card access system(s). Records are not limited to pedestrian traffic and may include vehicular traffic when there is an exit/entry at a parking gate.	Passive	Text/Logs
Location services	Wireless end-user devices may be tracked while on the University campus wireless network as a result of network security and wireless network management operations. While metadata about Internet activity may be tracked, the exact nature and content of the activity is not.	Passive	Telematics/ Location/GPS
Location services	End-user device location tracking occurs in order to relay geographical information to emergency responders in the event of 9-1-1 and campus security calls.	Passive	Telematics/ Location/GPS

Location services	Location tracking occurs when the virtual walkhome feature is activated by the user from the University's campus safety mobile app.	Active	Telematics/ Location/GPS
Communications			
Telephones	Telephone conversations may be recorded, where the individual is part of a service unit, or engages in contact center operations, for quality control & customer service training. Telephone calls may be recorded for safety and security investigations or the normal discharge of university operations. An announcement alerting the parties of the recorded call will be played back before the recording starts.	Active	Audio
Telephones	Call accounting (call duration, source, destination, costs etc) may be recorded for usage & license management and for reconciliation of long distance charges with the service provider(s).	Passive	Text/Logs
Telephones / Call center operations	Agent performance metrics (e.g calls dropped, answered, busy/talk-time, call duration) for service units that use a contact center may be recorded and reviewed by service managers for the purpose of quality control and to maintain proper contact center operations.	Active	Text/Logs
Email & chat	Email and chat monitoring (volume and metadata of email and chats, not the content) may occur for usage management and allocation of computing and digital storage resources.	Passive	Text/Logs
Computer monitoring & business systems			
Category	**Summary of monitoring activities**		**Type of record**
Internet traffic	Internet and local network traffic tracking occurs for bandwidth allocation and network capacity planning.	Passive	Text/Logs

Workorder/Request management system	Agent performance metrics may be tracked to assess completion time, volume and types of requests, to maintain a list of billable hours for external clients and to inform standards, policies, procedures and the creation of service level agreements.	Active	Text/Logs
Point-of-sales & campus oneCard			
Category	**Summary of monitoring activities**		**Type of record**
Print and copy management	Print and copy accounting is recorded. The location, volume and types of documents are recorded for usage management.	Passive	Text/Logs
Food and oneCard	Electronic cash registers and product-scanning systems may record purchases.	Passive	Text/Logs

4.3 Right to information

4.3.1 An employee may, upon request, ask the custodian of the recorded / monitoring data (e.g department head or appointed designate) for additional details, samples, copies of events and activities or general information regarding the use of the data. Such a request will not be reasonably withheld. A request under this clause is limited to an Employee's own data and captured events and activities.

4.4 Privacy

4.4.1 Access to recorded activities and events, under the custody and control of the University, is limited to officers and directors that are deemed to be data custodians under the

University's *Policy on Access to Electronic General and Personal Information*, or as defined by the University storage and records management standards, or as is deemed necessary and proper in the discharge of the University's function.

4.4.2 While the University does not subscribe to a "right to erasure / right to be forgotten" policy at the time of the approval of this document, it is committed to granting such requests, within the scope of records, activities and events that were collected and recorded as part of the employer's electronic monitoring, for employees that change or cease their relationship with the University, where technical and operational controls permit it and where the request is based on reasonable grounds.

4.5 Data Retention

4.5.1 In order to comply with the *Freedom of Information and Protection of Privacy Act, 1990* and other statutory requirements, all records, activities and events recorded using electronic monitoring within the scope of this policy, shall be kept for a minimum of one (1) calendar year from the date that the data was first captured.

4.5.2 Additional retention and data disposition schedules are applicable provided that it is in compliance with clause 4.6.1. Data may, in absence of a set disposition schedule, be kept in perpetuity as the employer sees fit to maintain proper University operations and functions or for quality control purposes.

5. Related policies

Laurentian University Policy on Freedom of Information and Protection of Privacy

Laurentian University Policy on Access to Electronic General and Personal Information

Laurentian University Policy on Managing Confidential Digital Information