ST. JEROME'S UNIVERSITY

Electronic Monitoring Policy

Institutional Manual
Approving Authority: Office of the President
Established: August 2023
Date of Last Review/Revision: November 9, 2023
Office of Accountability: Executive Director, Finance and Administration
Administrative Responsibility: Human Resources

Policy Statement

St. Jerome's University is committed to providing a place of employment that is safe, healthy, and respectful for all employees. We prioritize the health and well-being of all employees, including respecting, and protecting employees' privacy.

St. Jerome's University is committed to transparency with regard to electronic monitoring. The purpose of this Electronic Monitoring Policy (the "Policy") is to provide transparency about the University's use of electronic monitoring tools for employee activity.

Scope

This Policy is intended to outline the University's electronic monitoring practices and should be read in conjunction with any relevant and applicable legislation, including the *Electronic Monitoring Provisions of the Employment Standards Act, 2000 (ESA)* and *Ontario's Freedom of Information and Protection of Privacy Act, R.S.O. 1990 (FIPPA)*, as well as other applicable University policies, guidelines or standards, including but not limited to:

University of Waterloo Electronic Monitoring Guideline
St. Jerome's University Academic Staff Association Full-time Collective Agreement
St. Jerome's University Academic Staff Association Contract Academic Staff Collective Agreement

Nothing in this policy is intended to amend or supersede any grievance procedure or other aspect of any applicable collective agreement, employment contract or University Policy.

This policy applies to all employees as defined by the ESA. For clarity, "employee" under this Policy means those employees of the University who are considered employees under the ESA, including staff, faculty, contract academic staff, teaching assistants, research assistants, and casual staff.

Principles

The guiding principles for this policy are:

- St. Jerome's University uses electronic monitoring for the purposes of safety, information security, and resource management.

- Electronic monitoring data are to be used for the purpose for which the data are collected, in the proper discharge of the University's business, and operational functions.
- The use of electronic monitoring data beyond the purpose for which the data are collected is prohibited, except as outlined by this policy.
- The University does not actively monitor employees using electronic means for the purpose of employee performance management and discipline as a normal course of business.

Application

1) Electronic Monitoring Practices

a) "Electronic Monitoring" refers to digital collection of information which provides information about employee activity in physical spaces and on the digital network. The University uses various electronic monitoring tools in different circumstances and for different purposes.

b) The following tables outline how and in what circumstances St. Jerome's University and University of Waterloo use electronic monitoring tools, and the purposes for which information obtained through electronic monitoring tools may be used by the University:

Table 1: Electronic Monitoring at St. Jerome's University

Data Collected	Purpose	Information Steward
Electronic key/fob swipe for building access	Physical Security	Executive Director, Finance and Administration
CCTV/Video Camera Systems (in high traffic areas)	Safety & Physical Security	UW Special Constable Services
System login activity	Network Security	Executive Director, Finance and Administration
Casual/hourly employee time tracking	Payroll	Supervisors
Credit card transactions	Financial management	Director, Finance and Accounting

Table 2: Electronic Monitoring at University of Waterloo

Data Collected	Purpose	Information Steward
Watcard/Keyfob swipe for building access (excluding Residence)	Physical Security	University Secretary
Server and application access and activity (e.g., Office365, LEARN and Workday) from any Internet connected device at any location	Service Management Information Security	Chief Information Officer
Software use on university desktop computers, including mobile devices, at any location	Service Management Information Security	Chief Information Officer
Telephone records	Financial management	Chief Information Officer
Video surveillance	Safety & Security	University Secretary
Library card scan	Library resource management	University Librarian
University network activity	Network Security	Chief Information Officer

Wireless network activity (including campus location data)	Service Management Network Security	Chief Information Officer
Athletics facility use records **All other Watcard use**	Resource management Security	AP, Students
Employee time tracking	Payroll	Department heads
P-Card transactions	Financial management	Director of Finance
E-commerce (University as the merchant)	Authenticity of financial transactions	Director of Finance
Telematics from fleet vehicles at any location	Environmental sustainability	Executive Director of Plant Operations Director of Sustainability
Link tracking from university communications	Management of communications effectiveness	VP, University Relations

c) Data from electronic monitoring will generally only be used for the purpose for which the data are collected. Electronic monitoring data may be used in exceptional circumstances (e.g., law enforcement matters, emergencies or critical situations affecting individuals or public health and safety), in accordance with Ontario privacy legislation. Electronic monitoring data will not be used to actively track and monitor employees for the purposes of performance management or discipline, although such data may be used to verify performance management or disciplinary issues which are independently discovered or suspected, including issues discovered or suspected through the course of permitted or required uses of the data.

d) Electronic monitoring data may also be used for other purposes permitted or required by law, including conducting workplace investigations to ensure the University complies with statutory obligations. The University's use of any electronic monitoring tools for employment-related purposes is further subject to any rights an employee may otherwise have per their employment contract, collective agreement, or otherwise at law.

e) Electronic monitoring data will not be disclosed to anyone except those persons who are authorized by the appropriate information steward and appropriately trained, who need it in the performance of their duties and where disclosure is necessary and proper in the discharge those duties, or those requiring it for a legitimate purpose as provided for in this policy.

f) This Policy does not provide employees any new privacy rights or a right to not be electronically monitored. Nothing in this Policy affects or limits the University's ability to conduct or use information obtained through electronic monitoring.

g) All information collected through electronic monitoring will be securely stored and protected. In the event the University collects any personal information, as defined in *FIPPA*, when using the electronic monitoring tools listed in Tables 1 or 2, the University shall collect, use, disclose, retain, and dispose of personal information in accordance with applicable legislation, including, but not limited to, *FIPPA*.

2) Reporting Concerns

If you are concerned about employee surveillance, you should report those concerns immediately to your supervisor or appropriate leader. If it is not appropriate to report your concerns or issues to your supervisor or appropriate leader, or the matter is not resolved by doing so, you should direct your concerns or issues to your senior leader or Human Resources**.** Employees will not be subject to reprisal for reporting, in good faith, such concerns as outlined above or for inquiring about, exercising, or attempting to exercise any rights as provided under the ESA.

3) Support Resources

The following resources are available to assist all employees with understanding the application of this policy:

Executive Director, Finance and Administration
Director, Systems and Information Technology
Director, Human Resources

4) Posting, Notice, and Retention

a) The University will provide all current employees with access to or a copy of this Policy within 30 calendar days of implementation.

b) The University will provide all employees hired after this Policy is first implemented with access to or a copy of this Policy (or the applicable revised version) within 30 calendar days of the employee's start date.

c) In the event this Policy is amended, the University will provide each employee with access to or a copy of the amended Policy within 30 calendar days of the date the amendment(s) become effective.

d) The University shall retain a copy of this Policy and any revised version of this Policy for a period of three (3) years after it ceases to be in effect.