Policy Name:	Policy on Electronic Monitoring
Originating/Responsible Department:	Human Resources
Approval Authority:	Senior Management Committee (SMC)
Date of Original Policy:	September 28, 2022
Last Updated:	N/A
Mandatory Revision Date:	September 28, 2027
Contact:	Assistant Vice-President (Human Resources)

Purpose:

Pursuant to the requirements of the Ontario *Employment Standards Act, 2000* ("ESA"), Carleton 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. **The University does not actively electronically monitor employees for the purpose of employee performance management as a normal course of business.**

Scope:

This policy applies to all employees of the University, as defined by the ESA. For clarity, "employee" under this Policy means only those employees of the University who are considered employees under the ESA.

Electronic Monitoring Practices

The University uses various electronic monitoring tools in different circumstances and for different purposes. **The University does not actively electronically monitor employees for the purpose of employee performance management as a normal course of business.**

The University categorizes its electronic monitoring practices into two groups:

> Active Electronic Monitoring: is the use of electronic monitoring tools that are intended to intentionally track employee activity or location and is monitored in real-time or in close proximity to the time of collection.
>
> Passive Electronic Monitoring: is the collection, analysis and/or retention of data that may include, without limitation, data about employee activity or location either in physical spaces or on the university's network that is not actively monitored.

Active Electronic Monitoring of Employees

As a regular course of business, the University does not actively electronically monitor employees for performance management. The University reserves the right to actively electronically monitor employees for the purpose of employee performance management when there are reasonable grounds, with oversight from appropriate authorities, and in compliance with relevant legislation, University policies and collective agreements. Employee performance management may include tracking employee attendance, location, and activities to ensure fulfillment of their job duties and/or compliance with organizational policies. Examples of active electronic monitoring of employees may include, but are not limited to:

Monitoring the date and time of access to physical locations and digital resources.

Monitoring internet resource requests.

Monitoring physical location using global positioning system (GPS) technology such as in two-way radios for employee safety purposes.

Active electronic monitoring of employees may also include direct access to the contents of assigned account(s) and/or the device(s) used by an identified employee. University accounts include, and are not limited to, email, voicemail, Teams, SharePoint, OneDrive and other storage space assigned for use by an individual employee.

Passive Electronic Monitoring

The University conducts passive electronic monitoring of physical spaces and digital identities, assets, and resources for the following purposes:

- **Physical security** – To assure the safety of community members and the physical security of premises; to monitor for violations of organizational policy; and, to monitor for violations of municipal, provincial, or federal laws.
- **Environment management** - To assess and manage the physical environment, including but not limited to heating, cooling, lighting, and other facilities services that contribute to a comfortable living and workspace.
- **Information technology service assurance** – To identify indicators of service degradation, and to assure ongoing availability and integrity of digital assets and resources connected to the network.
- **Cybersecurity** - To detect, prevent, and respond to cybersecurity events and incidents, and to assure the security and safety of digital identities, assets, and resources.
- **Audit and compliance** - To monitor and assure confidentiality and compliance with organizational policies, contractual obligations, relevant legislation, and regulations.

Data collected during passive electronic monitoring may include data about identifiable employees. Such data may be used to review the activities of an identifiable employee or may be correlated with other data sets to review the activities of an identifiable employee.

The use of data collected during passive electronic monitoring at the University is done with oversight from appropriate authorities and in compliance with relevant legislation and University policies. The University has reserved, but is not limited to, the following electronic monitoring rights:

- To collect data relating to activities on university premises and on the university network that may be attributable to identifiable persons.
- To use the data for the purpose of assuring safety, security, and comfort within physical and digital spaces on university premises, and for other uses deemed appropriate and necessary.
- To use the data for the purpose of assuring the availability, integrity, and confidentiality of digital assets and resources connected to the university network or otherwise provided by the university, and for other uses deemed appropriate and necessary.
- To retain data for use as evidence in investigations, for business continuity or employee performance management purposes, or for other uses deemed appropriate and necessary.

In addition to the purposes listed in Appendix A, the University *may* use any electronic monitoring tools for the purposes of monitoring, evaluating or investigating employee performance, behaviour or conduct, including employee discipline. 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.

Business and Operational continuity

The University may use data that has been retained from passive electronic monitoring or may directly access information from university assigned account(s) and/or device(s) of an identified employee for the purpose of assuring business and operational continuity.

When an employee retains information related to university business operations or the operation of their department, unit, or team within their university-assigned account(s) and/or devices, and that employee is not available to retrieve the information, the University may directly access the account of the employee with oversight from appropriate authorities and in compliance with relevant legislation, and University policies and applicable collective agreement requirements.

General

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

In the event the University collects any personal information, as defined in the *Freedom of Information and Protection of Privacy Act* (FIPPA), when using the electronic monitoring tools listed in Appendix A, the University shall collect, use and disclose personal information in accordance with applicable legislation, including, but not limited to, FIPPA.

Posting, Notice and Retention

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

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.

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.

The University will provide a copy of this Policy to assignment employees assigned to perform work for the University within 24 hours of the start of the assignment or within 30 days of the Policy's implementation, whichever is later.

The University shall retain a copy of this Policy and any revised version of this Policy for a period of five (5) years after it ceases to be in effect.

Implementation, Review and Amendment

This Policy may be amended from time to time at the University's sole discretion. In the event that the University amends this policy, it will post and provide an amended copy of the Policy to employees within 30 days of the changes being made.

The Assistant Vice-President, Human Resources is responsible for periodic review and implementation of this Policy. Amendments to this Policy other than those set out in the paragraph below shall require the approval of the Senior Management Committee. The Assistant Vice-President, Human Resources may amend this Policy in order to update the following information contained herein:

a. the designation, title or identity of officials, offices, or departments and contact information within the University;
b. the title or citation of legislation, regulations, policies or procedures;
c. the Repository of Electronic Monitoring Tools at Appendix 'A'.

The Assistant Vice-President, Human Resources may establish, amend, abrogate or make exceptions to procedures for purposes of the effective implementation of this Policy, provided that such procedures or exceptions are consistent with the provisions of this Policy.

Contacts:

Assistant Vice-President (Human Resources)
Deputy Provost (Academic Operations and Planning)

Links to related Policies:

This Policy is intended to outline the University's electronic monitoring practices and should be read in conjunction with other applicable University policies, guidelines or standards, including but not limited to:

Acceptable Use Policy for Information Technology
Access to Information and Privacy Policy
Acquisition-of-Wireless-Cellular-Services
Card Access to Buildings and Labs Policy
Cloud Computing Security Policy
Data and Information Classification and Protection Policy
Desktop and Laptop Computer Equipment Policy
Email Use Policy

Hazard Reporting Policy
Information Security Incident Response Policy
Information Technology (IT) Security
Mobile Technology Security Policy
Password Policy for Information Systems
Remote Network Access Policy
Student and Visitor Trespass from University Property Policy
Student Communication Policy
Survey Policy
Video Recording and Surveillance Policy

APPENDIX "A"

REPOSITORY OF ELECTRONIC MONITORING TOOLS

The following Table outlines how and in what circumstances the University uses electronic monitoring tools and the purposes for which information obtained through electronic monitoring tools may be used by the University:

Category	Sub-Category	How Monitoring occurs and Purpose
Physical Security	Physical/electronic access tools such as FOBs, identification cards, badges and key cards	Access and egress from secured campus locations is controlled using card swipe and/or PIN. This records the dates, times, and locations an individual has entered facilities.
	Intrusion Alarms	Secured facilities are equipped with an alarm system that, if not disabled using an authorized individual's credentials, will alert Campus Safety Services to a possible intruder.
	License plate/parking enforcement	Parked motor vehicles in parking lots across campus are verified by Campus Safety Services to ensure parking regulations, including holding a valid parking permit, are complied with.
	CCTV Video Camera Systems and video	CCTV footage is used to identify threats to the safety of individuals on campus or threats to the buildings on campus. CCTV and video footage may also be used to support investigations of unlawful activity, health and safety, breach of contract, law or non-compliance with university policies.
Network Security	Virtual Private Networks (VPN)	Network security tools are used to ensure that the university's digital assets are protected from unauthorized access and to deter, detect and remediate cybersecurity incidents. The data gathered from these tools are passively monitored to detect possible cybersecurity activities and risks. These tools are deployed at both the individual device/workstation level and on an enterprise-wide basis for all active networks and data repositories.
	Anti-virus/malware	
	Web Gateways	
	Firewalls	
	IT security software /cybersecurity prevention tools and software (including spam/phishing emails)	
	Endpoint threat detection and response protection tools	
	Employee mobile device	

	management	
	Network and server logs	
Network and Systems Tools	Wireless internet	ITS monitors university-issued and personally enabled devices connected to the wireless internet on campus to identify anomalies in network traffic that may indicate a cybersecurity incident.
	Forensic tools	Forensic tools are deployed to identify issues with IT-related systems, associated software and cybersecurity. This may be used to assess compliance with university policies.
	Web analytics	Web analytics are used to passively monitor website traffic of an individual who has visited university-managed websites. This identifying information is limited to IP addresses.
	Data tools	Data management software assists with the proper allocation of digital storage based on existing and forecasted use. This may be used to assess activity or compliance with university policies.
	Mobile Devices/Two-way Communications Devices	Some mobile devices and two-way radios have a location or GPS-enabled feature which Is primarily used for individual safety. The location information, with other information, may also be used to assess activity levels of employees.
	Vehicle telematics / GPS in campus vehicles	On-board sensors detect and report on vehicle location, driver behavior (hard braking, rapid acceleration, etc.) and engine diagnostics. This is used to manage fleet assets and assist with vehicle occupant safety and security.
	Wi-fi location	ITS uses Wi-fi signals on campus to identify network segments that require additional capacity.
Computer Software	Email tracking software, associated systems and applications such as chats and collaboration tools	The software records copies of all messages sent or received by addresses within the University's domain to comply with recordkeeping and legal disclosure requirements such as a FIPPA request or a subpoena.
	Internal enterprise management software and applications (e.g., finance, HR tools)	Enterprise management tools that contain human resources or financial information are monitored to protect against unauthorized access to or loss of Confidential/Sensitive information. This may be used to assess compliance with legal requirements and university

		policies.
	IT and Facilities support and ticketing systems (e.g., remote desktop support, ITS Service Desk)	Ticketing systems are used to assign and track the completion of tasks to employees. This may be used to assess activity levels. ITS remote desktop support activities monitor employee behaviour while actively troubleshooting IT-related issues directly with the affected employee. The employee is notified at the time a remote connection is made and must consent through system prompts.
	Learning Management Software, and access logs related to these software	Mandatory training for employees is tracked using the university's Learning Management System to ensure training is completed as required by law and university policy. Employees involved in course design or delivery will have their activities logged by the Learning Management System. This may be used to assess activity levels or to ensure compliance with university policies.
	Other education-related tools, including proctoring software and access logs related to these software	Employees involved in the live, remote proctoring of an exam will have their actions recorded throughout the duration of the exam. This may be used in the event of an allegation by a student about the conduct of the examination.
Productivity Tools	Mobile and other telephony devices	University-issued or personally enabled mobile devices connected to university systems or software may be used to access any of the electronic monitoring tools identified.
	Library and research applications	Library and research software is used to track academic and scholarly works, publications and research proposals. This may be used to monitor compliance with research funding obligations, to assess compliance with university policies, and to assess activity for Tenure, Promotion and Confirmation purposes.
	Software for specific purposes (e.g., invoice management tools, queuing software)	Some software designed for a specific purpose, such as invoice management or queuing systems, may be used to assess activity levels in any particular business area.