715 Electronic Monitoring Policy

Effective: October 2022

The University of Guelph 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.

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;
- Privacy and Access to Information Guidelines;
- Confidentiality of Personal Information Policy;
- Video Surveillance System Policy;
- Computing Acceptable Use Policy and Guidelines
- Data Storage Guidelines

Application

1. This policy applies to all employees, as defined by the Ontario *Employment Standards Act, 2000* ("ESA"). For clarity, "employee" under this Policy means only those employees of the University who are considered employees under the ESA.

Electronic Monitoring Practices

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

3. "Electronic Monitoring" refers to employee monitoring that is done electronically.

4. The following Table (Figure 1) 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:

Electronic Monitoring Tools and Purposes	Electronic Monitoring Tool	Circumstances in Which Electronic Monitoring May Occur	How Electronic Monitoring Occurs	Purpose(s) For Which the Collected Information May Be Used
Vehicle telematics / GPS	All fleet and/or university vehicles during use	On board sensors detect and report on vehicle location, driver behaviour (hard braking, rapid acceleration, etc.), attached equipment operation and		Fleet management, driver safety and security, service delivery location and timing.

Electronic Monitoring Tool	Circumstances in Which Electronic Monitoring May Occur	How Electronic Monitoring Occurs	Purpose(s) For Which the Collected Information May Be Used
		engine diagnostics. For more information see our Vehicle Telematics Policy.	
IT security software	Continuous	Software tracks and triggers events for suspicious or risky user activity.	Network security
Email tracking	Continuous	Software records copies of all messages sent or received by addresses within the University's domain.	Network security
Electronic key fob/access badge systems	Each scan	An electronic sensor creates a record each time an authorized user scans their key fob and enters the University's premises or shared computers	Facility and network security.
Firewalls/VPN/Web Gateways	Continuous	Network security programs and tools to monitor the use and access of University systems and networks.	Network security
Endpoint threat detection and response protection tools	Continuous	"ETDR" monitors the use of workstations (programs run, files read and written, etc.) and compares it against a baseline to detect abnormalities and potential unauthorized use.	Network security
CCTV/Video Camera Systems (property and facilities, license plate recognition)	Continuous	Cameras record video footage and/or photo snapshots of specific areas and motor vehicle license plates for tracking authorized/unauthorized use of parking spaces within the University's properties and facilities.	Facility security, employee and asset protection, and service delivery.
Video surveillance (investigation)	With reasonable grounds to suspect unlawful activity or breach of contract	Private investigators may be retained to document employee activity outside of work using video camera technology.	To detect unlawful activity or activity in breach of the employment contract
RFID Tags (Equipment)	Continuous	Sensors attached to key pieces of equipment detect and report on equipment location	Asset Protection
Laboratory information and workflow management systems (Lab Services)	Continuous	Systems track the movement of materials and processes.	Materials tracking and productivity monitoring
Learning management and collaboration software and tools	Continuous	Software monitors access and use.	Service delivery and productivity monitoring.
University mobile device management	Continuous	Devices log calls, user information and activity.	Network Security

https://www.uoguelph.ca/hr/715-electronic-monitoring-policy-faqs [1]

5. In addition to the purposes listed in Figure 1, the University *may* use any electronic monitoring tools for the purposes of monitoring, evaluating or investigating employee performance, behaviour or conduct, including whether to issue an employee discipline, up to and including termination of employment. The University values employee privacy and its use of any electronic monitoring tools for employment-related or disciplinary purposes is discretionary. 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.

6. 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.

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

8. 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 Figure 1, the University shall collect, use and disclose personal information in accordance with applicable legislation, including, but not limited to, FIPPA.

Posting, Notice and Retention

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

10. 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.

11. 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.

12. 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.

13. 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.

Amendments

14. 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 provide an amended copy of the Policy to employees within 30 days of the changes being made.

Please refer to the FAQ page [1] for answers to common questions regarding this policy.

Page category: Policy [2]

Source URL:https://www.uoguelph.ca/hr/715-electronic-monitoring-policy

Links
[1] https://www.uoguelph.ca/hr/715-electronic-monitoring-policy-faqs [2] https://www.uoguelph.ca/hr/page-category/policy