NIPISSING UNIVERSITY

Policy Category:	General
Policy Number:	1.14.2022.U
Policy Name:	Electronic Monitoring Policy
Responsible Department:	Vice-President, Finance & Administration
Original Approval Date:	October 2022
Approval Authority:	Vice-President, Finance and Administration
Last Reviewed/Updated:	April 2023
Next Review Date:	October 2025

Nipissing 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.

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 the Access to Information and Protection of Privacy Policy and Procedures, the Acceptable Use Policy, and the Respectful Workplace and Learning Environments Policy.

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.

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

4. Appendix A 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:

5. 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 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. The University will provide affected employees with prior or post notification of the use of information, as outlined in Appendix A, in nonstandard situations.

7. 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.

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

9. 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

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

11. 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.

12. 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.

13. 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.

14. 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

15. This Policy may be amended from time to time in 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.

Appendix A

Electronic Monitoring Tool	**Circumstances in Which Electronic Monitoring May Occur**	**How Electronic Monitoring Occurs**	**Purpose(s) For Which the Collected Information May Be Used**
IT security software	Continuous	Software tracks and triggers events for suspicious or risky user activity.	Network security (e.g., block suspicious logins from out of country)
Email tracking	Continuous	Software stores all messages sent or received by addresses within the University's domain.	Network security (e.g., mass phishing attack mitigation)
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.	Facility security (e.g., identify/block unauthorized access to an area)
Firewalls/VPN/Web Gateways/network and application logging	Continuous	Network security programs and tools to monitor use and access of University systems and networks, including Blackboard, WebAdvisor, MS 365, etc.	Network and application security (e.g., identify/block unauthorized access to the network)
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 (e.g., identify/block a file containing malware)

Electronic Monitoring Tool	**Circumstances in Which Electronic Monitoring May Occur**	**How Electronic Monitoring Occurs**	**Purpose(s) For Which the Collected Information May Be Used**
CCTV/Video Camera Systems (facilities)	Continuous	Cameras record video footage of specific areas within the University's facility.	Facility security, employee, and asset protection (e.g., investigate vandalism)
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 employment contract (e.g., investigate theft)
Endpoint management solutions	Continuous	Solutions can identify an asset's location, logins, hardware specifications, and software installed.	Endpoint security (e.g., identify obsolete hardware)