McMaster University

Policies, Procedures and Guidelines

Complete Policy Title:

Electronic Monitoring Policy

Policy Number (if applicable):

Approved by:

Presidents and Vice-Presidents

Date of Most Recent Approval:

October 4, 2022, effective October 11, 2022

Date of Original Approval(s):

October 4, 2022

Supersedes/Amends Policy Dated:

Responsible Executive(s):

Assistant Vice-President & Chief Technology Officer (CTO)

Assistant Vice-President & Chief Human Resources Officer (CHRO)

Policy-Specific Enquiries:

University Technology Services

Human Resources Services

General Policy Enquiries

Policy (University Secretariat)

DISCLAIMER: *If there is a discrepancy between this electronic policy and the written copy held by the policy owner, the written copy prevails.*

PREAMBLE

1. McMaster University values employee privacy and is committed to transparency about electronic monitoring. The purpose of this Electronic Monitoring Policy (the "Policy") is to clarify the University's use of electronic monitoring tools for employee activity.

APPLICATION

2. This Policy applies to all McMaster University **employees** and **assignment employees**.

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

4. Nothing in this Policy is intended to amend or supersede any grievance procedure or other aspect of any applicable collective agreement, including the *McMaster Revised Policy and Regulations with Respect to Academic Appointment, Tenure and Promotion (2011)* and the *Supplementary Policy Statements*.

5. Employees and assignment employees working offsite at locations other than University property may also be subject to electronic monitoring by the host organization(s). The University may receive information from those organization(s), which it will treat in accordance with this Policy.

TERMS AND DEFINITIONS

6. For the purpose of interpreting this document:

   a) **Assignment employees** are individuals employed by a temporary help agency and assigned to perform work on a temporary basis for McMaster University.

   b) **CCTV** means closed circuit television surveillance system;

   c) **Electronic monitoring** refers to employee monitoring that is done electronically;

   d) **Employees** include only those individuals who are considered employees of the University under the *Employment Standards Act,* 2000 (the "Employment Standards Act"). This includes faculty, staff, members of the Management Group (TMG), postdoctoral fellows, sessional faculty, teaching and research assistants, clinical faculty, librarians, employees who are members of a bargaining unit, and interim employees. It also includes employees in supervisor roles (e.g., directors, chairs, deans).

ELECTRONIC MONITORING PRACTICES

7. The University uses various electronic monitoring tools in different circumstances and for different purposes.

8. The University categorizes its electronic monitoring practices into two groups:

   a) **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. For example, active electronic monitoring tools may include:

      (i) GPS and campus vehicle telematics;

(ii) CCTV video systems in specific University-owned and/or operated property and buildings, as described in the *Closed Circuit Television Surveillance Policy*;

(iii) Digital tools used for employee daily health screening and *Vaccine Policy* compliance (e.g., MacCheck);

(iv) Building and room access control systems for highly secure areas.

b) **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. Examples of passive electronic monitoring tools may include:

(i) Building and room access control systems ("swipe card access") for areas not considered highly secure;

(ii) Activity logs from software applications, networks, and servers;

(iii) Email, appointment, and meeting calendaring software.

9. ***Appendix A: Repository of Electronic Monitoring Tools*** outlines how, in what circumstances, and for what purposes the University uses electronic monitoring tools.

10. In addition to the purposes listed in *Appendix A*, at its discretion, the University *may* use electronic monitoring tools for monitoring, evaluating or investigating employee performance, behaviour or conduct, or ensuring compliance in completing required training (e.g., health and safety). These purposes also include informing decisions to issue discipline up to and including termination of employment. The University will conduct any monitoring, evaluation or investigation in compliance with relevant legislation and University policies.

11. 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 policies and legislation, including, but not limited to the University's *Notice of Collection* and FIPPA.

POSTING, NOTICE, AND POLICY RETENTION

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

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

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

15. 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.

16. 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

17. 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 employees with access to the amended Policy within 30 days of the changes being made. Each date on which this Policy is amended will be recorded and retained on its cover page, under the heading "*Supersedes/Amends Policy Dated:"*

APPENDIX A: REPOSITORY OF ELECTRONIC MONITORING TOOLS

This appendix may be updated from time to time based on the University's use of electronic monitoring tools.

Category	Sub-Category	Passively or Actively Monitoring Employees	Purpose of Monitoring **Any tool may be used for investigation or disciplinary purposes*	How Could Monitoring Take Place?
Computer Software	Communication and collaboration tools, including MS Teams, Zoom, , live chats and/or chatbots (e.g., Comm100).	Active	Collected data are only used for communication, collaboration, and business productivity purposes and not for employee monitoring. Occasionally, attendance at meetings taking place over Zoom or MS Teams is recorded, as it would be in an in-person setting.	Access and usage logs
	Communication and collaboration tools, including email, calendaring software (MS Outlook), and official University social media accounts.	Passive	Collected data would only be used actively for specific investigative purposes, including personal safety. Infrequently, and upon senior executive approval, collected data may be used actively for business continuity purposes (i.e. email, calendaring software) upon a staff departure.	Access and usage logs
	Support and service provision software (e.g., live chat, IT or HR support ticket system). Also, the features integrated into service provision software intended to capture client satisfaction ("rate your experience").	Both Active and Passive	To be responsive to the service provider's clients, collected data are used for service improvement and to support ongoing program development. Also, data are used to prepare staff training programs to address a range of client issues. Collected data are not used to monitor employees.	Chat logs, ticket history logs, and communication /support logs. Satisfaction data are aggregated and analyzed at a high level.
	Internal enterprise management software and applications (e.g., finance, HR tools, daily health screening).	Passive	Collected data would only be used actively for specific investigative purposes.	Access and usage logs
	Learning Management Software, and other education-focused software tools.	Passive	Collected data would only be used actively for specific investigative purposes.	Access logs
	Proctoring software.	Active monitoring for student/learner; passive monitoring of employee.	Collected data are only used for educational purposes and not for employee monitoring.	Usage logs
Productivity Tools	University-owned mobile and telephony devices.	Passive	Collected data would only be used actively for specific investigative purposes.	Usage logs and billing history

Category	Sub-Category	Passively or Actively Monitoring Employees	Purpose of Monitoring *Any tool may be used for investigation or disciplinary purposes*	How Could Monitoring Take Place?
	Employee mobile device management software.	Passive	Collected data would only be used actively for specific investigative purposes.	Location history
	Registration tools for special events, learning, and professional development activities.	Passive	Passive monitoring tool and may be used to track employee attendance or activities. Post-activity data may be reported to third parties for employees subject to professional regulation.	Access and usage logs
	Business productivity software with cloud integration (e.g., MS O365).	Passive	Collected data would only be used actively for group task completion or specific investigative purposes.	Access and usage logs, shared document files
Research Tools	Data collection software including survey software, statistical software, etc. with named licensing.	Passive	Collected data would only be used actively for specific investigative purposes.	Access and usage logs
	Time management applications (e.g., QuickBooks) for tracking fee-for-service billing or compliance reporting.	Passive	Collected data would only be used actively for specific investigative purposes.	Access and usage logs
	Research instrument or core facility usage tracking.	Passive	Collected data would only be used actively for specific investigative purposes.	Access and usage logs
	Monitoring tools for specific equipment and facilities for safety compliance.	Passive	Passive monitoring tool used for tracking compliance and could be used for investigative purposes.	Access and usage logs
Network Security Tools	Network monitoring tools and server logs including wireless internet access points.	Passive	Used for network issue diagnosis process. Collected data would only be used actively for location identification in extreme emergency cases.	Event logs
	Forensic tools	Passive	Used to alert administrators when unusual behaviour on the network is detected, and diagnostic processes are required. Collected data would only be used actively for investigative purposes.	Event logs
	Website analytics	Passive	Collected data are gathered for aggregate statistical purposes and not for any other purpose. Provides data of when, where, and how users engage with website properties.	Website usage logs

Category	Sub-Category	Passively or Actively Monitoring Employees	Purpose of Monitoring **Any tool may be used for investigation or disciplinary purposes*	How Could Monitoring Take Place?
Cyber Security Tools	Virtual Private Networks (VPN)	Passive	Data used to authenticate access to University systems. Data would only be used actively for investigative purposes.	Access and usage logs
	Firewall and Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).	Passive	Used to alert administrators when unusual behaviour on the network is detected, and diagnostic processes are required. Collected data would only be used actively for investigative purposes.	Event logs
	Cybersecurity prevention system tools and software, including anti-virus/malware, and endpoint protection software.	Passive	Used to alert administrators when unusual behaviour on the system is detected, and diagnostic processes are required. Collected data would only be used actively for investigative purposes.	Event logs
Physical Security	Perimeter access to buildings and interior room doors. Proximity ID card readers for access control; used with employee identification cards, badges, key cards, FOBs, etc.	Both Active and Passive	Tool authenticates access to buildings. Data may be used actively for highly secure areas on campus to ensure that only approved persons gain entry to these areas. Otherwise, data are collected passively and would only be used for investigative purposes.	Access control logs
	Transponder-based parking lot access control system.	Passive	Used to control access to University parking properties and for parking fee enforcement. Could be used for investigative purposes.	Access by individuals is passively monitored. Only lot capacities are actively monitored.
Location	Video surveillance systems including CCTV (Closed Circuit Television).	Both Active and Passive	Security and safety of campus community, property, and assets. The majority of monitored data are passively collected and actively monitored data are not specific to employees. All data passively collected would only be used for investigative purposes.	*See Closed Circuit Television Surveillance Policy.*
	GPS in campus vehicles.	Active	Actively monitored data are only used during snow removal events to estimate progress for campus safety. Passively collected data are not used.	Real-time monitoring of vehicles using GPS during snow removal activities.

APPENDIX B: RELATED POLICIES AND LEGISLATION

This Policy is intended to outline the University's electronic monitoring practices and should be read in conjunction with the following policies, statements, and collective agreements. Any question of the application of this Policy or related policies shall be determined by the Assistant Vice-President & Chief Human Resources Officer (CHRO) or the Assistant Vice-President & Chief Technology Officer (CTO), as appropriate, and in conjunction with the administrator of the other policy or policies. The University reserves the right to amend or add to the University's policies and statements from time to time (this is not a comprehensive list):

- Closed Circuit Television Surveillance Policy
- Data and Information Classification Policy
- *Employment Standards Act*, 2000, S.O. 2000, c. 41
- *Freedom of Information and Protection of Privacy Act* (FIPPA)
- Handling of Personal Information, Policy for the
- Information Security Policy, including Acceptable Use of University Computing Resources
- McMaster University Revised Policy And Regulations With Respect To Academic Appointment, Tenure And Promotion ("Tenure and Promotion Policy"), 2011; and associated Supplemental Policy Statements (SPS)
- McMaster Parking Services Regulations
- *Personal Health Information Protection Act* (PHIPA)