FAQs - Electronic Monitoring Policy

1. Why is this policy being implemented?

The Ontario government recently passed Bill 88, Working for Workers Act, 2022. This Bill amends the Employment Standards Act, 2000 (ESA) and requires employers with 25 or more employees to have a written policy with respect to electronic monitoring of employees in place by October 11, 2022.

2. What is the purpose of the Electronic Monitoring Policy?

This policy is to clarify the University's use of electronic monitoring tools for employee activity and ensure transparency about electronic monitoring that is undertaken by the University.

3. What does this policy change for me as an employee?

There will be no changes to the electronic monitoring practices currently in place. McMaster's practices have been consistent with the new government requirements outlined in the policy.

4. What is outlined in the Employment Standards Act, 2000 (ESA), with respect to electronic monitoring of employees?

The Policy must include:

- A description of how and in what circumstances the employer may electronically monitor employees;
- The purposes for which the information obtained through electronic monitoring may be used by the employer;
- The date the Policy was prepared; and
- The date any changes were made to the Policy.

In addition, the ESA requirements:

- Do not establish a right for employees not to be electronically monitored by their employer; and
- Do not create any new privacy rights for employees.

5. What electronic monitoring occurs at the University?

Many electronic systems, tools and software support the safety, and smooth operation of the university. Some tools collect a broad range of information as part of their typical operation such as swipe card access, GPS tools, digital communication tools and CCTV video systems, which may be logged or archived. While McMaster does not usually use these tools to actively to monitor its employees, the University maintains its ability to access this data should it have reason to review any issues of concern.

Employees are encouraged to familiarize themselves with the Electronic Monitoring Policy that includes a repository of electronic monitoring tools at the university.

6. Can McMaster look at my work emails and documents?

All documents saved on the institutional servers or in the cloud are University property, and this includes any documents or attachments on an employee's Microsoft 365 account. The university does not actively monitor McMaster email accounts or business productivity software.

These items could be accessed with appropriate authorization for investigative purposes only.

Additional information around the use of accounts and resources which are connected to McMaster's network can be found in the Information Security Policy.

7. I use a university owned mobile device. Will McMaster be able to access my personal emails or information?

McMaster does not have the ability to access employees' personal email accounts (Gmail, yahoo accounts etc.). McMaster does not have access to any personal passwords, login information or any personal applications.

Anyone using a McMaster device must ensure that it is being used for appropriate purposes.

8. Will Zoom or Microsoft Teams meetings be monitored?

McMaster does not actively monitor or record any Zoom or Microsoft Teams meetings, but there may be recordings made by meeting facilitators of various sessions in support of learning or sharing of information amongst teams and across the community. If there was an incident that required investigation, and if there was a recording made of the meeting that was relevant, it could be accessed and used as part of that review.

9. What is the difference between active electronic monitoring and passive electronic monitoring?

The University has made a distinction between *active* and *passive* electronic monitoring in the policy.

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 close to real time. This includes GPS, room access controls for high security areas, CCTV video systems, and some communication and collaboration tools.

Passive Electronic Monitoring is the collection, analysis and/or retention of data that may include data about employee activity or location either in physical spaces or on the University's network that is not actively monitored. This includes swipe card access, activity logs for software applications and networks, and email and meeting calendaring software.