UNIVERSITY OF
ST. MICHAEL'S COLLEGE
IN THE UNIVERSITY OF TORONTO

ELECTRONIC MONITORING POLICY

Policy Owner: Bursar & CAO
Date of Policy: September 27, 2023

1.0 PURPOSE

The University of St. Michael's College (USMC) is committed to transparently sharing the University's electronic monitoring practices.

2.0 APPLICATION

This Policy applies to all University employees, including Faculty, Directors, Managers, and Senior Leadership. The Policy is intended to outline the University's electronic monitoring practices and should be read in conjunction with other University policies, guidelines or standards, including but not limited to:

- University of Toronto's Appropriate Use of Information and Communication Technology https://www.provost.utoronto.ca/planning-policy/information-communication-technology-appropriate-use/; and
- University of Toronto's Guideline: Email Accounts for University of Toronto Staff, Faculty and Librarians https://people.utoronto.ca/wp-content/uploads/2020/02/Guideline-Email-Accounts-for-University-of-Toronto-Staff-Faculty-and-Librarians.pdf

3.0 POLICY

The use by employees of USMC assigned devices and associated services are solely intended for the purpose of carrying out USMC business. This includes all electronic communications, e-mail, voicemail, and other communications and information transmitted or received over USMC's systems. USMC maintains the right to enter its systems, and to monitor, inspect, review, copy, delete, retain, and/or disclose any electronic communications or other information maintained on or transmitted over USMC systems.

Employees should not assume that any electronic communications or other information transmitted or received over USMC systems are private or confidential or that USMC or its designated representatives will not access and review the communications and information.

The above services undergo continual preventative maintenance and performance tuning which involves traffic logging.

Although certain applications may be password-protected, such protection is for the security of USMC information, and should not be understood as providing employees with individual privacy. Individuals using USMC equipment should have no expectation of privacy, and no expectation that any information stored on its systems—whether the information is contained on a computer hard drive, computer disks, personal folders or files, or in any other manner—will be private. Employees should not use USMC e-mail, electronic communication systems, or other systems to send, receive or store messages not related to USMC's business that the employee wishes to keep private, personal or confidential.

In the event of a conflict between the terms of this policy and those of another USMC policy, contract, collective agreement, law or regulation, the provisions of the latter shall prevail.

4.0 ELECTRONIC MONITORING PRACTICES

a) USMC periodically checks traffic and communications on its network and technology systems without notice to ensure system-wide compliance with USMC policies.

b) USMC reserves the right to monitor activity logs on its network and subscribed cloud services to conduct health checks of its IT services, to ensure appropriate use, to evaluate efficiency and efficacy, to prevent and detect security breaches, high risk and malicious activity, for research and other legitimate purposes.

   Those logs include:

   - Networks and systems (e.g., email and Internet usage, network logins, application usage, equipment sensors, network threat detection tools).
   - Cell phone voice and data usage to minimize overage charges.
   - Malware infections and risky behaviours such as visiting websites and opening attachments from external sources to protect data and physical assets.
   - VPN connections and the originating IP address to detect cyber-attacks from outside Ontario.

c) External monitoring outside of USMC control includes:

- Technology vendors monitor activity according to their terms of use agreement and relevant privacy legislation. Vendors' customers do not have visibility to these data. Examples:
  - Cellular tower traffic
  - GPS data from Google Maps
  - Microsoft Office 365 Insights providing personalized work recommendations

d) USMC does **not** on a regular basis track and/or monitor the following employee activities:

- Access and attendance (e.g., key fobs, electronic timecard systems)
- Location (e.g., GPS tracking of devices)
- Surveillance (e.g., video or audio recording, keylogging)
- Cell phone voice calls (e.g., voice calls recording)
- Employees private files
- Emails and/or chats

USMC does not conduct active monitoring of employees' activities using its platforms in the normal course of business. The activity logs may be used after-the-fact for formal investigations to support organization decisions or external litigation. In extraordinary circumstances, electronic surveillance may be authorized if there are reasonable grounds to believe that misconduct is taking place and other investigative measures are ineffectual.

Information collected will be used only when there is sufficient evidence of workplace violations, illegal activities or where law enforcement or judicial inquiries require the University to release its information. If any information collected under this policy is used for a formal investigation or to support internal decisions, USMC would have had reasonable grounds to necessitate such an investigation, and the information will be disclosed to the employee within the investigation process.

5.0 IMPLEMENTATION

a) The University shall provide an electronic copy of this policy to all current employees of the University within 30 days of implementation.

b) Any new employee will be informed of the existence of this policy at the time of hire.

c) Employees will be notified within 30 calendar days of any changes to this policy.