Electronic Monitoring Policy

Purpose/Intent

The Alma Mater Society of Queen's University values trust, discretion, and transparency and believes employees deserve to know when and how their work is being monitored. This policy is to fulfil the 2022 revisions to the Employment Standards Act (2000).

Terminology

The term "AMS" means the Alma Mater Society of Queen's University Incorporated and the Alma Mater Society of Queen's University.

The term "Electronic Monitoring" means using technological, electronic, or digital means to track, observe, or monitor someone's actions.

The term "Personal Information" means any factual or subjective information about an identifiable individual.

Scope

This policy applies to all AMS employees.

Policy

Electronic Monitoring Practices

1. Alma Mater Society of Queen's University collects information through electronic monitoring for a variety of reasons, including protecting the company's legal and business interests. The company will electronically monitor the following activities and procedures:

    a. Email and file storage systems in Microsoft 365
    b. Desktop and Laptop devices (we do not monitor daily user activity, but we do monitor system statistics and location for asset protection and remote support)
    c. Network activity and cloud platforms for security purposes.
2. Software monitoring will occur only through the applications that fall under the AMS ecosystem (such as Email, Teams, SharePoint, OneDrive, and Business Central for example). These will be monitored on personal devices, but the personal devices

themselves, including the contents and data stored in those devices, cannot be monitored.

3. Any information collected by electronic monitoring may be used during employee reviews or during consideration of disciplinary decisions.
4. To promote impartiality, and to ensure any information collected through electronic monitoring is handled appropriately, Alma Mater Society of Queen's University will monitor these activities by:
    a. Only leveraging monitoring tools for support, and security purposes.
    b. Maintaining an ethical stance by respecting personal privacy as much as possible.
    c. Not hindering user experience with the monitoring tools and software. These tools are used to aid in supporting users, and as a result, users will not need to take any additional action for these tools to work properly.

Privacy and Confidentiality

1. The AMS's monitoring is aimed at collecting information related to its operations and business. However, some information collected by electronic monitoring may be considered personal information. When personal information is under Alma Mater Society of Queen's University control, it is the responsibility of the company to protect it.
2. All information collected through electronic monitoring will be securely stored and protected. If any personal information is collected, its use and disclosure will be limited to achieve the stated purpose of its collection. The AMS will adhere to all privacy and confidentiality legislation that applies to the collection, use, and disclosure of personal information obtained by electronic monitoring.

Information Digital Protection Mechanisms:

1. The AMS reserves the right to access any/all digital information within our ecosystem in the event of a suspected breach. This is to isolate, contain, and further protect both personal and proprietary organizational data during an ongoing investigation.
2. In the event of a suspected security incident, the AMS, as a best practice, will typically temporarily disable/suspend access to the suspected account(s) until a thorough investigation by the Information Technology Officer can be completed and any/all suspected account(s) cleared for further use. Typically, in these scenarios, the user(s) affected will be notified by alternative methods with the next steps or conclusions of the investigation before resuming access.
3. The AMS remains committed to operating in as narrow a scope as possible when auditing information to ensure that ONLY the information accessed will aid in the investigatory process. Findings from the investigation could lead to further

collaboration with the Human Resources Office and a continuation of the investigation. If further action is required on a specific account(s), the other accounts cleared of the initial investigation process will be reinstated to minimize operational impact

Monitoring

Monitoring for compliance with this policy will be carried out by…

Responsibility and/or contact person	Human Resources Office and Information Technology Office
Approved by	Board of Directors
Date initially approved	September 25, 2022
Date last revised	April 12, 2026
Related policies, procedures, and guidelines	Employment Standards Act
Policies superseded by this policy	N/A