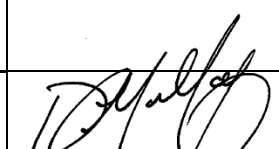


POLICY TITLE: Electronic Monitoring Policy	POLICY SECTION: Human Resources & Information Technology Services	POLICY NO: 2.4
RELATED BOARD POLICY:	1.2.2 Recruitment, Retention and Turnover 1.4.5 Regulatory and Legislative Compliances	
RELEVANT LEGISLATION:	Ontario Employment Standards Act	
PRIMARY APPROVER:	President	
SECONDARY APPROVER:		
RESPONSIBLE AUTHORITY:	Human Resources	
DATE APPROVED:	November 29, 2022	
DATE(S) REVIEWED / REVISED:	November 29, 2022	
POLICY REVIEW - FREQUENCY:		
APPROVER SIGNATURE(S):		

It is not the intention of King's University College to explicitly monitor an employee's activity or participate specifically in the surveillance of their actions. The following policy outlines how information is collected and where at times this may be required.

1. Purpose

1.1. King's University College (King's) values trust, discretion, and transparency and believes employees deserve to know when and how their work is being monitored. This policy is to be used in addition to the Information Technology Services Acceptable Use Agreement, Video Monitoring Policy, and Email Policy for Students and Employees, and is intended to establish guidelines for King's practices and procedures related to electronic monitoring of employees.

2. Scope of the Policy

2.1. This policy applies to all employees and departments of King's University College.

3. Definitions

3.1. **Electronic monitoring:** Using technological, electronic, or digital means to track, observe, or monitor someone's actions.

3.2. **Personal information:** Any factual or subjective information about an identifiable individual.

4. Policy

- 4.1 King's University College does not intentionally monitor employees but has systems in place to collect information through passive electronic monitoring to ensure legislative and legal compliance, data security, workplace safety, and information technology and network uptime and improvements. King's will electronically monitor the following activities and procedures:
- 4.1.1 Suspicious or risky user and/or computer activity that may result in viruses, malware, security breaches, and/or inadvertent information disclosure. This monitoring is based on patterns of activity or evidence of a security breach and not related to websites or software utilized by employees, faculty, or students.
 - 4.1.2 User access logs, successful and unsuccessful, on computers, web applications, and websites are recorded and electronically monitored for suspicious activity. This data is used to prevent security breaches and ensure data security. The content of websites access or applications used is not monitored.
 - 4.1.3 Software copies of all email messages sent or received by addresses within the King's University College's domain are retained in the event of disclosure for legal requirements and/or operational continuity. The content of emails is not monitored.
 - 4.1.4 Mobile device management can be used to access the location of a College-owned mobile device in the event of theft, loss, or unauthorized use. If necessary, management software can be used to wipe the contents of the device.
 - 4.1.5 Access to parking lots and buildings when a parking fob or employee card is used. Data may be used for troubleshooting access or activity review.
 - 4.1.6 Public areas are covered by a video camera system that is reviewed for security purposes relating to damage, harassment, and/or other unauthorized activities.
 - 4.1.7 King's, with guidance from the Director of Human Resources or the President, 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. Any information collected by electronic monitoring may be used during employee reviews or during consideration of disciplinary decisions.
- 4.2 To promote impartiality, and to ensure any information collected through electronic monitoring is handled appropriately, King's University College will monitor these activities in accordance with:
- 4.2.1 Existing collective bargaining agreement, employment contracts, and the Employment Standards Act (ESA)

4.2.2 The provisions of collection, use, and disclosure of personal information as defined in the Freedom of Information and Protection of Privacy Act (FIPPA)

5. Privacy and Confidentiality

5.1. King's monitoring is aimed at collecting information related to the educational and organizational directives, strategic plan and core values. However, some information collected by electronic monitoring may be considered personal information. When personal information is under King's University College control, it is the responsibility of King's to protect it.

5.2. 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. King's will adhere to all privacy and confidentiality legislation that applies to the collection, use, and disclosure of personal information obtained by electronic monitoring.

6. Appendices

None