Status: Final

Electronic Monitoring Policy

Approved By: Chief Administrative Officer

Approved On: October 6, 2022

Policy Statement

A policy setting out details regarding the Region's electronic monitoring of its employees and contractors.

Application

This policy applies to all employees and contractors who use technology resources and assets during employment.

Purpose

York Region is committed to maintaining a transparent workplace for all employees and contractors.

While performing work-related duties and activities, employees and contractors are entrusted with the use of technology resources and assets. There is a legislated obligation for the Region to outline when employees and contractors are electronically monitored, how the information is collected and for what purposes.

The goal of this policy is to increase awareness of a person's "digital footprint" (record of online activity and user authentication), and the potential uses of this information.

Definitions

Electronic Monitoring: All forms of monitoring of employees and contractors that is done electronically.

Assets: All Region owned/leased facilities, vehicles, and technology.

Technology Resources: Region owned or supplied equipment, applications or services used to input, store, process, transit, and output information such as:

- Equipment: End user devices (computers, laptops, tablets, smartphones, cellphones), peripheral devices (monitors, docking stations), computing equipment (servers, storage), printers and removable media (USB memory sticks)
- Applications: On-premises and cloud-based software applications and systems
- Services: Network and remote access services, wired and Wi-Fi services, cellular services (voice and data), internet services, and voice telecom services

Personal Technology: Any technology not provided by the Region, such as computers, laptops, tablets, smartphones, printers, and internet services.

User Activity: Traceable electronic user data, such as sign in, sign out date and time stamps, data entry, device usage, information accessed and browsing history.

Authentication Information: Unique information used to accurately identify a user for the purposes of granting access to a technology resource, such as usernames and passwords, PINS, and hardware tokens.

Third-Party Systems: Applications not owned by the Region, where Regional users retrieve information, enter information, or create transactions.

Description

All employees and contractors may be electronically monitored when using the Region's technology resources and assets at any physical location. This includes both Regional worksites and home office locations.

As stated in the Code of Conduct, communications over the Region's electronic networks and any data obtained from the use of a Region asset should not be considered private.

Active Monitoring

The Region actively monitors assets in real-time for physical safety, the protection of assets, dispatching of services, complaint resolution, investigative purposes, and adherence to Regional policies. Active monitoring may also be legislatively required, depending on the circumstances.

Examples of active monitoring include:

- Regional buildings and locations actively monitored by card/badge access, electronic keys, or security cameras

- Fleet vehicles equipped with automatic vehicle locator (AVL) and Global Positioning System (GPS) technology
- Transit vehicles equipped with security cameras
- Electronic cabinets/lockers and lock boxes
- Dispatch and call centre use of performance management and incident replay software

Employees and contractors are made aware of active monitoring by posted signage, written consent, acceptable use agreements, or recorded messaging (*i.e., "This call may be monitored for quality assurance purposes").*

Access to real-time monitoring as well as its user activity data and recordings is considered private and restricted to specifically authorized staff.

Technology Resources Monitoring

Any equipment, application or service that requires a Region login creates traceable data through user activity. This may include certain third-party systems. Access to employee and contractor user activity data is considered private and restricted to specifically authorized staff.

Examples include:

- User authentication information
- Desk phone and softphone
- Remote access – VPN, Citrix
- Office applications
- Business software

Examples of third-party systems include:

- Financial institutions
- Provincial and federal systems
- Cellphone providers
- Fuel providers

Purposes of User Activity Data

Information gathered by electronic monitoring activities may be used for purposes such as:

- Physical safety
- Optimization of service delivery
- Training and quality assurance
- Complaint resolution
- Protection of assets

- Auditing and legislative requirements
- Investigation of alleged violations of law, regulations, or applicable Regional policies, procedures and expectations or other instances of suspected misconduct

Responsibilities

Employee and Contractors

- Adhere to the standards and behaviour outlined in all Regional policies
- Seek clarification when uncertain about information included in this policy
- Notify their Supervisor/Manager if they suspect a policy breach

Supervisors/Managers

- Adhere to the standards and behaviour outlined in all Regional policies
- Take appropriate corrective actions in the event of policy violations
- Consult with People, Equity and Culture when required

People, Equity and Culture

- Develop, maintain, and annually review this policy
- Ensure existing employees and contractors are provided a written copy of this policy within 30 days of the policy date
- Distribute this policy to new employees and contractors on or before their start date
- Provide consultation and advice on the interpretation of this policy
- Respond to inquiries related to the policy

Regional Management Team

- Advise People, Equity and Culture of new technology or changes in technology usage that may monitor employee and contractor activity

Compliance

While performing work-related duties and activities, Regional employees and contractors are to comply with all Regional policies, laws, regulations, government guidelines and internal controls.

Any questions regarding the interpretation and or application of a Regional policy are to be directed to the employee’s Manager, HR Consultant, or IT Services.

Reference

Legislative and other authorities

- Employment Standards Act, 2000
- Working for Workers Act, 2022
- Municipal Freedom of Information and Protection of Privacy Act
- Personal Health Information Protection Act, 2004

Related policies

- Code of Conduct
- Corporate Privacy Policy
- Corporate Asset Management
- Information Management Policy
- Acceptable Use of and Management of Technology Policy

Contact

HR Support Centre, People, Equity and Culture, Office of the CAO

Approval

CAO Signature: ORIGINAL SIGNED BY BRUCE MACGREGOR Approved: October 6, 2022

Accessible formats or communication supports are available upon request.

#14240052