CORPORATE POLICY

THE CITY OF
Waterloo

Policy Title: **Use of Technology with Monitoring Capabilities**
Policy Category: **Administration Policy**
Policy No.:   A-038
Department: Corporate Services
Approval Date: October 3, 2022
Revision Date: N/A
Author: Natalia Chebel
Attachments: N/A
Related Documents/Legislation:
          Employment Standards Act, 2000, SO 2000, C.41
          Municipal Freedom of Information and Protection of Privacy Act,
          R.S.O. 1990, c. M.56
           Communication Technology Use Policy
          A-010 Information Security Policy
          A-002 Social Media Policy
          H-004 Employee Code of Conduct
          Communication Technology Use Policy
          Corporate Procedure - Email Usage Standards and Procedure
          Corporate Procedure - Information Security Incident Management
          Process
          Procedure for Privacy Impact Assessment (PIA)

Key Word(s): electronic monitoring; privacy; business activity

POLICY STATEMENT:

The City of Waterloo is committed to maintaining a transparent, fair and secure
workplace. This commitment continues to be demonstrated through fulfillment of its
obligations under the amendments introduced to the *Employment Standards Act* on
April 11, 2022. Where the City employs technology with monitoring capabilities, the City
commits to informing City staff, Councillors, volunteers and contractors about:
- how and in what circumstances such technology is used;
- the purposes for which the information obtained through the use of such
  technology may be used; and
- any changes made to this Policy.

PURPOSE:

The purpose of this Policy is to:
- ensure that the City of Waterloo meets its legislated responsibilities under the *Employment Standards Act*, *Municipal Freedom of Information and Protection of Privacy Act* and other applicable legislation;
- inform City staff, Councillors, volunteers and contractors of the current use of technology with monitoring capabilities, as well as purposes, for which this technology is used;
- establish principles the City will follow when developing and implementing technology with monitoring capabilities.

DEFINITIONS:

Active Directory is a Microsoft service that allows the management of the authentication and authorization of users and machines on a network.

Disclosure (of personal information) means releasing or making the information available to an individual or organization.

Technology with Monitoring Capabilities means technology that may collect information about employees' activities, communications, location and/or productivity, while employees conduct City business. Such technology may include but is not limited to a computer, telephone, radio, camera, access control systems, GPS, etc.

Employee, for the purposes of this Policy, will include the categories of persons identified by the *Employment Standards Act as "employees"*, as well as City Councillors, volunteers and contractors.

Personal Information means recorded information about an identifiable individual, such as (but not limited to):

- Names,
- Race, gender and gender identifiers (use of pronouns, collection of gender based-data), sexual orientation, national and ethnic origin,
- Residential street addresses,
- Telephone numbers,
- Email addresses,
- Marital/relationship/family status,
- Views and opinions,
- Opinions of others about the individual,
- Descriptions of activities/location of person/use of property,
- Images of persons,
- Images of use of property (e.g. photos of the inside of homes),
- Financial activities (payments and purchases),

- Medical information (e.g. medical history, health status, description of injuries, diagnosis, and treatment).

Privacy means a set of interests and rights that an individual has regarding their ability to control the collection, use, disclosure and retention of their own personal information that is in the custody or control of a third party. Privacy is not an absolute right in all situations. Personal information may be collected, used, disclosed or retained without the consent of individuals where specific legislation permits.

Privacy Impact Assessment (PIA) is a comprehensive assessment of a project or a system that identifies the impact that the project or system might have on the privacy of individuals, and sets out recommendations for managing, minimizing or eliminating that impact.

Telematics is a wireless device that includes global positioning systems, designed to record data through the vehicle's onboard computer and transmit the captured data to a central application.

Use (of personal information) means viewing or dealing with the information in a manner that does not include disclosing it.

Web Filter is software that monitors and manages the locations where users are browsing on the Internet, enabling to either allow or block web traffic in order to protect against potential threats and enforce corporate policies.

SCOPE:

This Policy applies to employees (as defined in the *Employment Standards Act*), members of Council, contractors and volunteers.

POLICY COMMUNICATION:

This policy will be made available to employees through the City's website, intranet, and email. A physical copy of the policy will be posted on bulletin boards in staff access areas of City facilities and will be provided to employees upon request. The policy will be provided to new employees within 30 calendar days of the day the individual becomes a City employee.

POLICY:

1.0.   TECHNOLOGY WITH MONITORING CAPABILITIES

The City may use technology with monitoring capabilities which may collect information about employee activities, while employees conduct City business in City facilities and at other City property, use City devices and equipment, or work remotely, as permitted by law.

Technologies with monitoring capabilities the City currently uses are listed in Schedule "A" attached to this Policy.

This policy operates with and as a supplement to existing and future City of Waterloo Policies that may, from time to time, apply to employees and be related to this policy, including but not limited to:

- Communication Technology Use Policy
- A-002 Social Media Policy
- H-004 Employee Code of Conduct

2.0. PRINCIPLES

The City will adhere to the following principles when the implementation of a technology with monitoring capability is considered:

2.1. PURPOSE SPECIFICATION

Prior to implementing/utilizing a technology with monitoring capabilities the City will identify and communicate to employees the purposes of such implementation.

2.2. NECESSITY AND PROPORTIONALITY

To be considered necessary and proportionate, a technology with monitoring capabilities must meet the City's business needs and minimally impact employees' privacy. Where possible/appropriate, the City will avoid using invasive monitoring practices, e.g., the use of video surveillance in sensitive areas. Active monitoring of employees will be avoided unless required for a specific and lawful purpose.

2.3. INFORMATION PRIVACY

Where employees' personal information is collected as a result of the use of a technology with monitoring capabilities, the City will ensure that:
- collection of personal information is limited to what is necessary to fulfill an identified purpose;
- personal information is not used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law;
- personal information is retained only as long as necessary for the fulfilment of identified purposes;
- personal information is maintained as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used; and

- personal information is protected by appropriate security safeguards relative to the sensitivity of the information.

Prior to the implementation of a technology with monitoring capabilities, Privacy Impact Assessment will be conducted to ensure that the impact on employees' privacy is minimized and personal information is protected from inappropriate collection, use, disclosure and disposition.

2.4.   OPENNESS AND TRANSPARENCY

Where appropriate, the City will engage employee groups into the process of designing and implementing technologies with monitoring capabilities, and make information about such technology easily available and understandable.

2.5.   NON-DISCRIMINATION

Use of technologies with monitoring capabilities and analysis of information collected through these technologies will be fair, bias free and non-discriminatory.

The City will ensure that:
- biases are not introduced into the interpretation of monitored data;
- there is equality in the manner of data processing;
- one group is not subject to more intensive or punitive monitoring; and
- rules about how monitoring data are interpreted are applied consistently.

3.0.   REVIEW

Leadership and unions/associations will have the opportunity to participate in the review of the Policy. Future revisions to Schedule "A" attached to this policy will be approved by the Corporate Management Team and communicated to all employees (including Council members, contractors and volunteers).

4.0.   RULES AND PROCEDURES

The City will create rules and procedures the City will follow to implement this Policy.

COMPLIANCE:

In cases of policy violation, the City may investigate and determine appropriate corrective action.

Schedule "A"
Technologies with Monitoring Capabilities Currently used by the City
(Maintenance/Updates to the Schedule may be made by approval of the Corporate
Management Team)

Technology	How does monitoring take place?	Purpose
Email security solutions	Emails classified by the system as threats, as well as compromised email accounts may be isolated and accessed.	Protection of the IT infrastructure from threats coming from email. Defense against email fraud
Web filtering solution	Can be used to monitor employee browsing behaviours and activities on the web	Detection and prevention of web-based attacks on the IT infrastructure
Threat hunting solution (network security)	Data on employee desktops, laptops, cell phones, tablets, etc. may be analyzed for threats	End-user device protection from cyberthreats
Active directory auditing software (network security)	Employee logon activity (into the City's network) may be analyzed	Mitigation of the risk of access privileges violation
System audit logs	User interaction with applications/systems is captured by the majority City systems, including but not limited to logging in/out, accessing certain areas/modules of or records in an application, deletion or creation of records, altering a record, change of access rights, accessing/making changes to various control systems, etc.	Diagnosing and troubleshooting an issue; privacy or security (physical or cyber) breach investigation.
External call recording software	Content of employees' phone conversations with customers (in selected City divisions only)	Customer service quality assurance
Corporate electronic calendars (e.g. MS Outlook)	Information in shared or non-shared calendars may be accessed	Workload distribution, employee availability, ensuring office/shift coverage, estimated employee location in case of emergency
GPS - Global Position System (on City issued laptops and mobile devices)	GPS applications are installed on mobile devices and laptops carried by City employees to inspections and other off-site	Employee safety, capturing metadata for reports/images taken.

	activities. Location of devices, timing may be accessed	
Vehicle telematics / GPS	Hardware and associated software are installed on City vehicle. Monitoring occurs during on shift use. Some exceptional monitoring may occur during personal use (e.g., in case of an accident)	Fleet/asset management, driver safety and security, insurance claim processing, incident/accident/complaint investigation; work scheduling
Mobile data/phone use tracking	Usage reports are submitted to employees' supervisors for review (where applicable)	Ensuring appropriate usage of mobile data/voice/text plans
Time/task tracking tools (add on functionality to business systems, e.g. AMANDA, Maximo, Emergency Reporting System, or stand alone applications)	Time used to complete a task and tasks associated with a specific assignment are tracked. Entries are reviewed by employees' supervisors.	Benchmarking for staffing levels and workload; ensuring proper recording of activities; response/completion time tracking; payroll
Time self entry systems	Entries by employees are reviewed by supervisors. Employee specific reports by time code may be run and reviewed	Payroll, attendance management
Clock in/clock out system	Electronic records are created when employees enter a City facility at the beginning of the shift or leave it at the end of the shift (for participating employee groups)	Payroll, attendance management
Video surveillance on City property	Video surveillance occurs on a continuous loop, however authorized employees may access security footage when a specific incident occurs. Access to security footage may be granted to employees, other than those overseeing the video surveillance system, in limited situations only	Certain workplace investigations (e.g., workplace violence), security incidents involving City employee, specific case investigation by police
Physical Access Control Systems	People's movement on City properties through secured entrance points is captured	Physical security of property and people