BRAMPTON

COUNCIL POLICY

Category: Information and Technology

Electronic Monitoring Policy (Policy in effect, subject to Council approval)

Policy Number: ITS -110
Approved by: Council Resolution # Click or tap here to enter text.– Click or tap to enter a date.
Administered by: Digital Innovation & Information Technology and Human Resources
Effective Date: October 11, 2022

Policy in effect, subject to Council approval

1. Background

The Province of Ontario has introduced Bill 88, Working for Workers Act, 2022 that states that employers must have an electronic monitoring policy that must be instituted and communicated to all staff by October 11, 2022.

2. Purpose

The City of Brampton ('City') is committed to maintaining a transparent and fair workplace. In accordance with Bill 88, Working for Workers Act, 2022, the purpose of this Electronic Monitoring Policy is to serve as confirmation that the City logs and monitors the use of City resources. City resources are provided to staff to improve productivity of business operations, to deliver services for residents and to enhance the effectiveness of communications. This policy outlines what resources are monitored and how the information collected may be used by the City. The City may rely on such information obtained through electronic monitoring for implementing corrective measures, up to and including discipline.

3. Application and Scope

This policy applies to all City Staff and Elected Officials.

4. Policy Statements

4.1 Policy

4.1.1 All City owned and operated equipment has logging enabled and may be subject to monitoring. The information collected is monitored to support business operations, provide services to our residents, and protect the integrity of our Information Network. All information is securely stored within the City's Corporate Infrastructure. Users should

be aware that the information collected or generated, including but not limited to emails, documents, and instant messages created or transmitted through the City's corporate systems, remains the property of the City. The City recommends refraining from using Corporate Devices for personal use (refer to section 8.2 – IT Administrative Directive), however, should you choose to use Corporate devices for personal items, any personal information will be securely stored with the same standards as corporate data and considered the property of the City and will adhere to all retention by-law requirements.

4.2 Collection

4.2.1 The City collects the following data from IT Equipment:

a) Phone recordings (e.g. 311, Transit Call Centre, IT Service Desk, etc.) for quality assurance or safety/compliance reasons, in which case, staff and callers are made aware that the phone calls are being recorded.

b) Logons and logoffs on end user devices, servers, applications (including Cloud/SaaS applications), network and VPN

c) Logs of peripheral devices used on end user devices, such as storage devices (USB, DVD/CD, Tape, SD Card, etc.), wireless devices, communication ports, imaging devices and printers

d) File operations locally, on the network, in the cloud and on externally connected storage (files opened, copied, created, renamed, modified and/or deleted to/from these devices)

e) Internet usage data including URLs/domains, pre-defined website content category, web page headers, search engine queries, timestamps, bandwidth consumption, and browsing time

f) Application usage, including software downloads, actions performed within the application and timestamp of actions performed

g) Radio communication systems for Transit, Call Centre, Enforcement, Animal Services and Corporate Security for quality assurance, training and safety.

h) IP addresses, system information and timestamp of information technology resources connecting to or transmitting to/from the city network

i) Telephone and mobile phone summary data including inbound and outbound calls, time of call, call duration

j) Vehicles & Fleet Equipment

- Global Positioning System (GPS) location
- Usage (Fuel, Mileage)

k) Physical Facility Security Equipment

- Video surveillance
- Facility access (Key Fob/Access Card)
- Facility Controls (Lights, Temperature)

4.3 Usage

4.3.1 The City may use the information collected for the following purposes:

a) To detect abnormal activity and inform the City of a potential issue:

b) Service disruption (e.g. intensive query or report requests causing a system to slow down or become unresponsive)

c) Security threat (e.g. a specific user uploading 50,000 documents to an external website or email content containing malicious links),

d) Breach of a policy (e.g. accessing explicit material on a website)

e) Activities that cause the City to incur a financial cost or loss (e.g. roaming charges, high long distance)

f) To establish usage or trending dashboards or reports

g) Compliance (e.g. manage licensing, contract renewals or responding to audits requiring an understanding of user usage)

h) Operations (e.g. traffic patterns to understand peak usage time of a particular service, application or network)

i) As input to resolve a technical issue that requires troubleshooting of user access or system activity (e.g. user cannot connect to VPN, user did not receive an email, user cannot access a website or application, etc.)

j) As evidence for forensic investigation requested by the City or authorized 3rd party such as a law enforcement agency

k) As input to enforce security, detect unauthorized access or safeguard City personnel and assets

l) As input to enhance City services (e.g. find my plow)

m) In response to Freedom of Information Requests

n) In response to Litigations Requests

o) In response to any request flowing and in compliance with the "Requests for DI&IT Confidential Information SOP"

4.4 Retention

4.4.1 To ensure that all information collected is only kept for as long as it is required, the City of Brampton will retain the information collected in accordance with the City's Records Retention By-Law.

5. Roles and Responsibilities

5.1 All Staff

5.1.1 All City of Brampton staff and elected officials are responsible for:

a) Adhering to this policy and related policies;

5.2 Leaders

5.2.1 Leaders are responsible for:

a) Ensuring that all staff and users are informed of this policy;

b) Enforcing adherence to the requirements of this policy;

c) Taking appropriate corrective actions in the event of policy violations.

5.3 Digital Innovation & Information Technology Division

5.3.1 Management and staff of the Digital Innovation & IT Division are responsible for:

a) Developing and managing the policy in coordination with the Human Resource Division.

b) Providing interpretation and guidance in relation to this policy and any guidelines.

5.4 Human Resources

5.4.1 The Human Resources Division is responsible for:

a) Developing and managing the policy in coordination with the Digital Innovation & IT Division.

b) Provide guidance and assistance to staff and management in dealing with issues, non-compliance, and associated reporting in relation to this policy.

6. Compliance

6.1 Compliance

6.1.1 Information in the Users care may be subject to access requests under Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) or internal review in respect of any devices or systems they use in connection with City business. This process may extend to personal data and communications stored within the IT environment. If there are any other legitimate authorized reasons to do so, such as retrieving email, voicemail, or documents in the event of an unscheduled absence or unexpected departure from the City, the

appropriate approvals must be obtained using the Requests for DI&IT Confidential Information SOP.

6.1.2 Appropriate City staff who are governed by confidentiality agreements, may be authorized and/or required to access the information to meet legal obligations or if there are reasonable grounds to suspect a staff member has abused or contravened this policy. Any investigation into the use of IT Resources must be authorized according to the Requests for DI&IT Confidential Information SOP.

6.2 Consequences of non-compliance

6.2.1 Staff members in breach of this policy will be reported to the appropriate level of management, who may take remedial action up to and including dismissal.

6.2.2 Staff members who violate laws when using the IT environment may be subject to criminal and/or civil prosecution.

7. Definitions

7.1 **"City"** means the Corporation of the City of Brampton.

7.2 **"Computer Monitoring"** refers to the practice of collecting user activity data on City-owned computers, networks, and other IT infrastructure. This data includes, but is not limited to, web browsing history, files downloaded, data input, network traffic, logons to corporate systems, interactions with data, peripheral device usage, and information about the staff's end user devices.

7.3 **"GPS"** means global positioning system that consists of a network of satellites and receiving devices used to determine the location of a device (vehicle) on Earth.

7.4 **"Information Technology Resources"** refers to computers, printers, mobile devices (including smartphones and tablets), software, network resources (including Internet, messaging, and social media) and telephony (including voicemail).

7.5 **"Key Fob/Access Card"** is a small physical device provisioned to City staff and contractors that is used to unlock doors and gain physical access into City facilities.

7.6 **"Staff"** means all full time, part time, volunteer, and contract employees of the Corporation, including Mayors and Council office staff.

7.7 **"Vehicle Monitoring"** refers to the practice of collecting information on vehicle usage and may include GPS location tracking and fuel consumption.

7.8 "**Video Surveillance"** refers to surveillance by means of a camera that monitors or records visual images of activities on City-owned property.

8. References and Resources

This Policy should be read and applied in conjunction with the following references and resources as updated from time to time. Please note that some of the following documents may not be publicly available.

8.1 External references

- *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) R.S.O.1990 c.M.56*
- *Employment Standards Act, 2000*

8.2 References to related bylaws, Council policies, and administrative directives

- Use of IT Resources Admin Directive ITS-100
- Records Retention by-law 272-2014
- Employee Code of Conduct HRM-100
- Information Management Policy 14.8.1
- Privacy Administrative Directive - GOV-130

8.3 References to related corporate-wide procedures, forms, and resources

- Requests of DI&IT for Confidential Information

Revision History

Date	Description
2022/09/07	Policy Creation Date
2022/10/dd	New. Approved by Council Resolution #
2025/10/01	Next Scheduled Review *(3 years after approval)*