HR07 – ELECTRONIC MONITORING OF EMPLOYEES

Policy Type: Human Resources **Policy Number:** HR07 **Reviewed**: February 12, 2026

1.0 Purpose

The Stouffville Library Board values trust, discretion, and transparency and believes employees deserve to know when and how their work is being monitored. This policy is intended to establish guidelines for Stouffville Library practices and procedures related to electronic monitoring of employees.

2.0 Definitions

Electronic Monitoring is defined here as tracking employee location and/or activities through various electronic devices such as computers, cellphones, GPS systems, and more.

Employee means a person who works at the Stouffville Library, either part-time, full-time, or temporary.

Video Surveillance refers to surveillance by means of a camera that monitors or records visual images of activities on company-owned property. Video surveillance does not include the capture of audio.

Computer Monitoring refers to the practice of collecting user activity data on company-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 employee's computer.

Data Collection refers to the automated or manual processing of employee data. This includes the collection, use, and storage of employee data such as computer activity data and other forms of personal information.

Personal Use refers to an employee using company-owned devices, networks, and other assets for personal tasks such as non-work web browsing and sending personal emails.

Personal Information refers to any data collected about an identifiable individual. This includes obfuscated data that, when combined with other information, could identify the individual.

3.0 Policy

The Stouffville Library collects information through electronic monitoring for a variety of reasons, including protecting legal and business interests.

Employees should have no expectation of privacy in any content or correspondence created, transmitted, received, accessed, or stored on the Library's IT and communications systems or corporate-issued electronic devices, including through Internet access, on social media, or through remote access from non-work locations and through the corporate virtual private network (VPN). Employees should not use the corporate IT and communications systems or corporate-issued electronic devices for any matter that the employee wants to keep private or confidential from the organization.

The Library has the right, at any time when deemed necessary, to monitor and preserve any communications that utilize the corporate network in any way, including data, voicemail, telephone logs, internet use, network traffic, etc., to determine proper utilization, regardless of the ownership status of the mobile device used to access the corporate network.

4.0 Systems with Electronic Monitoring Capabilities

The Library engages in the electronic monitoring of employees as defined within this policy. Monitoring occurs on work-issued/networked hardware, Library owned/operated software/apps, public online platforms owned/operated by the Library, and social media platforms.

The Library currently makes use of the following systems that are capable of electronically monitoring and collecting information relating to employees or their use of these systems:

- Library network, hardware devices, and file storage and sharing systems
- Email accounts (includes individual accounts, shared accounts, and distribution lists that are issued and managed by the organization)
- Social media platforms, listservs, and message boards that the Library and/or staff participate in and/or post to
- Chat, instant messaging and videoconferencing services available to staff for work purposes
- Library website
- Video surveillance cameras that monitor the Library's interior, entrances/exits, and exterior property
- Library telephones and work-issued cell phones
- Scheduling, time and attendance, and training software

- Staff Intranet
- Integrated Library System
- Security systems at Library facilities (such as key card access points)

5.0 Use of Systems for Electronic Monitoring

The Library does not typically collect and review electronic data to monitor employees on a routine basis. The systems and programs that permit the Library to electronically monitor employees are intended primarily for the provision of services and productivity tools, and to meet technological infrastructure and security needs.

Although it is not the primary purpose, the Library may use any available forms of electronic data for the purposes of:

- Evaluating staff performance
- Identifying safety concerns
- Gathering information to analyze and improve Library operations and workflow
- Ensuring security of facilities
- Investigating complaints or suspected breaches of Library policy

In appropriate cases, the Library may rely on data/information gathered through the Library's electronic monitoring systems to investigate (formally or informally) and discipline employees.

6.0 Duties and Responsibilities

CEO

- Maintain Electronic Monitoring Policy
- Assist with interpretation and application of the policy

Employees

- Understand scope of this policy and how it applies to your employment
- Seek clarification if unsure about any information included in the policy
- Report concerns or ask questions regarding electronic monitoring

Information Technology

- Collects and maintains data associated with the secured network, the Internet, mobile devices (including BYOD), instant messaging, e-mail, and device tracking.

Facilities (Management)

- Maintains oversight of video surveillance technology including the collection and storing of data and content
- Maintains and negotiates contract with video surveillance vendors if required

7. Posting Notice and Retention

The Library shall provide a copy of this policy to each employee within 30 calendar days of its implementation or within 30 days after any changes made to this policy.

The Library shall provide a copy of this policy to all new employees within 30 calendar days of the employee commencing employment with the Library.

The Library shall retain a copy of this and any revised version of this policy for three years after it ceases to be in effect, or such other time as may be prescribed by legislation.

8. Related Documents

- HR10 - Use of Technology
- AP53 - Employee Code of Conduct
- AP62 - Digital Recording of Meetings
- *Employment Standards Act*
- *Occupational Health and Safety Act*