Section of Policy Manual: Personnel	Policy No. : PER-16
Subject: Electronic Monitoring of Employees	Policy Approval Date: October 20, 2022
Year of next review: October 2026	Last Review/Revision Date:

POLICY STATEMENT:

The Gravenhurst Public Library Board understands the importance of technological innovation in the delivery of our services. We strive to adopt new technologies where they enhance our operations and keep our employees safe. We also understand that any use of technology must be done ethically, responsibly, and respectfully.

PURPOSE:

To ensure that employees are aware of when and why the GPL Board engages in workplace electronic monitoring.

To outline the GPL Board's approach to electronic monitoring, which may be used to collect information about employee activities in the workplace.

APPLICATION

This policy applies to all GPL Board employees.

POLICY

Definitions

Electronic Monitoring means the GPL Board's collection of information about an employee's activities through employer-owned electronic devices such as computers, computer networks, cell phones, GPS units, communication radios, key FOBS, and time clocks.

Privacy Expectations and Responsibility
The GPL Board respects every employee's reasonable expectation of privacy and is committed to upholding protections of workplace privacy required by law.

Employees should have no expectation of privacy in any content created, transmitted, received, accessed, or stored on the GPL Board's IT and communications systems and GPS monitoring systems.

Employees should not use the GPL Board's IT and communications systems and GPS monitoring systems for any matter that the employee wants to be kept private or confidential from the GPL Board.

Employees are strongly encouraged to use personal devices (not connected to the GPL Board's networks) to conduct personal business during their scheduled work breaks since it may be difficult for the GPL Board to distinguish between personal business and GPL business when conducting electronic monitoring or reviewing stored information through employer-owned devices.

As GPL Board employees are expected to carry their GPL Board issued cell phones with them outside of regular business hours and while away from the office, reasonable personal use is permitted. In choosing to use the GPL Board issued phone for personal reasons an employee acknowledges that District IT Services staff will have access to their personal information. Personal data and information on the GPL Board issued cell phone, including but not limited to passwords, links to web sites, personal email, or social media sites, are visible to District IT Services staff.

Employees should be aware that all information on the cell phone is for public record and is the property of the GPL Board.

While Employees should have no expectation of privacy in the use of the GPL Board's IT and communications systems and GPS monitoring systems, any employee personal information collected in the process of monitoring will be used or disclosed only as required to protect the GPL Board's business interests and to meet its legal obligations, in compliance with and subject to applicable privacy laws.

Monitoring of Systems, IT and communications systems and GPS Monitoring Systems

The GPL Board monitors the access and use of its IT and communication systems, including its computers, networks, telephones, email, text messaging, voicemail and internet use, and its GPS monitoring systems, communication radios, key FOBS, and time clocks, as reasonably required to protect its business interests and to meet its legal obligations.

The following describes how, and in what circumstances, the GPL Board may electronically monitor employees, as well as the purposes for which the GPL Board may use the information obtained through electronic monitoring:

- Protecting the integrity of the GPL Board's IT and communications systems and GPS Monitoring Systems, including protection against computer viruses, damage to software or hardware, loss of GPL documents or information, and protecting against excessive telephone or computer usage;
- For the purposes of network and cyber security, on a continuous basis, the GPL Board IT Provider's automated software tools monitor the use of workstations and all incoming and outgoing network traffic, to detect abnormalities, report unusual activity, detect threats, and prevent potential unauthorized use. When personal devices, such as tablets or cellphones, download and use the GPL Board's applications, tracking is limited to the performance and operation of Town applications and work partitions;
- For the purposes of web-traffic filtering, on a continuous basis, the GPL Board IT Provider tracks user website browsing and activity on any GPL Board issued user computer;
- Protecting against unauthorized access or disclosure of the GPL Board's confidential information, proprietary information, or employee or third-party personal information in the GPL Board's control;
- Protecting employees against discriminatory, harassing, or violent behaviour from co-workers or third parties;
- May monitor the use of email, text messaging, and telephone systems to ensure that use is in accordance with this Policy;
- Finding lost messages or data, or to retrieve messages lost due to computer failure;
- Following up on pending matters left by former employees;
- Auditing the use of the GPL Board's resources;
- Assisting in investigations of alleged wrongdoing or violations of GPL Board policies;
- Complying with any other legal obligation;
- Monitoring facility access; or
- Monitoring productivity on an aggregate basis and timekeeping.

The GPL Board reserves the right to monitor any electronic activity on the GPL Board's servers or transmitted through the GPL Board's networks. In most instances, such electronic monitoring is carried out passively by automated software, and employee anonymity and individual privacy is maintained. In rare cases, where a threat or unusual activity is detected, an individual may need to review specific activity related to a specific device or user.

To achieve these purposes, the GPL Board may, in its discretion, access, intercept or review any information created on, transmitted to, received or printed from, or stored or recorded on the GPL Board's IT and communications systems and GPS monitoring systems.

The GPL Board may store copies of such data and communications acquired through monitoring for a period of time after they are created and may delete such copies from time to time without notice.

The GPL Board may, in its discretion, use information obtained through electronic monitoring to determine if there has been a violation of its policies. Where appropriate, such information may lead to disciplinary action, up to and including termination of employment, subject to applicable collective agreement provisions and applicable laws.

ADMINISTRATION:

A written copy of this Policy will be provided to Employees within 30 calendar days of being approved.

A copy of the written Policy will be provided to any new Employees within 30 calendar days of a new Employee being hired.

Should the Policy be amended, the GPL Board will provide a copy of the amended policy to Employees within 30 days of the changes being made.

Where an Employee has questions about this policy they may speak with the GPL CEO/Chief Librarian.

VARIATION OF THE POLICY:

The GPL CEO/Chief Librarian shall have the authority to revise, amend or remove the Electronic Monitoring of Employees Policy, provided the revision(s), amendment(s) or removal are in accordance with legislative requirements.

This Policy will, always, be applied in accordance with the applicable employment standards, occupational health and safety, and human rights legislation, as well as the collective agreement, where applicable.

EFFECTIVE DATE:

This policy takes effect immediately upon approval.

REVIEW:

This policy will be amended as required and approved by the GPL CEO/Chief Librarian, pursuant to legislative requirements.

Related Documents:

Written Policy on Electronic Monitoring of Employees (Government of Ontario)
Employment Standards Act, 2000
Municipal Freedom of Information and Protection of Privacy Act
GOV-14 Intellectual Freedom
PER-02 Staff Use of Technology
PER-03 Staff Use of Social Media