Electronic Monitoring Policy

Legal References: *Ontario Employment Standards Act, Occupational Health and Safety Act*, *Human Rights Code, Municipal Freedom of Information and Protection of Privacy Act*
Policy References: Stratford Public Library Staff Manual 2022

Policy Statement:

The Stratford Public Library will conduct its business in an accessible, clear and visible manner so that its activities are open to examination. The Library is committed to promoting a culture where employees and Library Board members are aware of and understand the principles of transparency as they pertain to electronic monitoring of information collected by the Library.

Purpose:

This Policy has been developed to explain the circumstances under which the Library may engage in electronic monitoring of its employees and Library Board members and the reasons why it may do so. This Policy also provides transparency about how the Library tracks employees and Library Board members use of Library electronic systems and devices.

Definitions:

"**Electronic Monitoring**" means collecting, recording, and reviewing electronic data.

"**Employee**" includes all permanent full-time, permanent part-time, temporary or casual employees, and any temporary employee who is employed by a temporary placement agency or contractor that has been assigned to perform work for the Library using its technology resources.

"Board Member" includes any current members of The Stratford Public Library Board.

"**Technology**" includes all computer equipment, personal computers, laptops, PDAs, tablet computers, voice messaging systems, servers, and mainframes that are owned or leased by the Library, including without limitation, any and all communications, content, documents, data, information and messages accessed, created, stored, sent, received or viewed using such equipment.

Scope:
This policy applies to all employees and Library Board members and they will receive a copy of this compliance policy.

Procedure:
The Library may engage in any of the following forms of electronic monitoring, from time to time:

What data/systems may be monitored?	Why is this data being monitored?	When may the Library monitor this data?	What purpose will the Library use this data?
The geographical location of any electronic device used to log on to the Library 's network and/or systems.	(a) Protect the integrity and security of the Library 's networks and systems (i.e. to determine whether an attempted log-in is suspicious—e.g. there is an attempted log-in from Sydney, Australia when the worker normally works in Stratford).	(a) Every time a device attempts to log on to the Library 's networks and/or systems.	(a) Safety and security; prevent unauthorized persons or organizations from accessing the Library 's networks and/or systems.
Digital files created and/or stored on the Library 's network / servers, including endpoint detection and response software logs for all new files created.	(a) Network security and integrity. (b) Ensure compliance with applicable Library policies, including but not limited to those related to workplace harassment, bullying, discrimination, and information	(a) All files are constantly scanned by the software and then reviewed if a suspicious file alert is received. (b) If the Library suspects a worker is or has violated an applicable Library policy.	(a) Safety and security; determine if files need to be removed from the Library 's network / servers and/or any further action is needed to secure and protect the Library 's networks and systems. (b) To follow the Progressive Disciplinary Policy.

What data/systems may be monitored?	Why is this data being monitored?	When may the Library monitor this data?	What purpose will the Library use this data?
	technology use.		
Emails sent from and to a Library email address; and, all written communications and documents stored, posted, sent and/or received on Microsoft Teams and Zoom (collectively, the "Communications").	(a) Protect the integrity and security of the Library 's networks and systems, including maintaining an audit trail of all Communications with compromised accounts (suspected or actual). (b) e-Discovery, compliance, and investigation purposes. (c) Back-up and recovery purposes. (d) Ensure compliance with applicable Library policies including, but not limited to, those related to workplace harassment, bullying, discrimination, and appropriate workplace communications.	(a) All Communications are stored and may be reviewed if the Library suspects that a worker's account has been compromised and/or they have been sent or have sent malicious content. (b) All Communications are stored and may be monitored if any of these events arise. (c) All Communications are stored and may be access and reviewed if Communications are deleted, erased, or otherwise removed from the Library 's systems. (d) If the Library suspects a worker is or has violated an applicable Library policy.	(a) Identifying any external breach of the Library 's networks; discipline up to and including termination of employment for cause. (b) Fact finding, disclosure and evidentiary purposes. (c) Ensure Communications can be recovered if deleted, erased or otherwise removed from the Library 's systems. (d) To follow the Progressive Discipline Policy
All internet traffic on the Library 's internet networks and/or servers, including internet browsing history on Library-owned	(a) Network security. (b) Ensure compliance with applicable Library policies, including but not limited to	(a) If there has been an attempt to access malicious, illegal or inappropriate websites (e.g. the black web, terrorist	(a) Identifying any external breach of the Library's networks; discipline up to and including termination of employment for

What data/systems may be monitored?	Why is this data being monitored?	When may the Library monitor this data?	What purpose will the Library use this data?
devices.	those related to workplace harassment, bullying, discrimination, and appropriate internet use.	sites, etc.) on the Library 's networks. (b) If the Library suspects a worker has or is violating applicable Library polices.	cause. (b) To follow the Progressive Discipline Policy
GPS location of Library-owned cell phones and vehicles.	(a) Protect the integrity and security of the Library 's networks/systems and property. (c) Check / confirm driver's speed.	(a) If the device or vehicle is, or is suspected to have been, lost or stolen. (c) If the driver is involved in a motor vehicle collision and/or if there are allegations that the driver was driving at an excessive speed.	(a) Recovery Library -owned property; and prevent external breaches of Library networks/systems. (c) Verification for insurance purposes
Cell phone call logs provided by the Library 's cellphone service provider.	(a) Fiscal responsibility.	(a) At time of billing.	(a) Ensure accuracy of billings before payment is made to the Library 's cellphone service provider.
Video surveillance cameras.	(a) Physical security of the Library 's premises, personnel, guests, physical resources, files, materials and vehicles.	(a) Constantly.	(a) Security; discipline up to and including termination of employment for cause.

Although every effort has been made by the Library to make an exhaustive list of the circumstances and purposes for which the Library may engage in electronic monitoring, there may be circumstances when the Library may, from time to time, engage in electronic monitoring not listed above and/or use the data collected for reasons and purposes not listed above.

The Library does not provide employees a guarantee to, or right of, privacy or confidentiality in connection with the use of any of the Library 's Technology including,

but not limited to email; Teams and Zoom messaging, audio or video calls; voicemail; internet connectivity; files created and stored. Employees should have no expectation of privacy in these communications.

Anything created, stored, accessed, sent or received is the property of the Library and, therefore, may be accessed or reviewed at any time by the Library, at its sole discretion, without further notice.

The Library reserves the right to examine or monitor any and all uses of its Technology including, but not limited to, the right to monitor, access, use and/or disclose all messages sent over email and/or other electronic communications for any purpose; all Internet addresses visited; and all material downloaded, uploaded or viewed by workers. Again, no notice will be given to any employee before or after such access.

Accessing and Correcting Personal information

The Library may unintentionally collect personal information, as defined in the *Municipal Freedom of Information and Protection of Privacy Act* (the "*MFIPPA*"), through electronic monitoring.

An employee or Library Board member may make a written request to the Library Administration requesting access to any records containing their personal information. The Library will provide the requesting employee or Library Board member access to such records subject to and in accordance with the *MFIPPA*. For clarity, the Library will not provide access to records, including records containing an employee's or Library Board members personal information, if such records fall outside of the application of the *MFIPPA* or the Library is otherwise entitled to refuse such access under the *MFIPPA*.

After having been given access to such records, the employee or Library Board member may, if they believe there is an error or omission in those records, make a written request to the Library Adminstration requesting that the information be corrected in accordance with the *MFIPPA*.

Legislative Authority:

The Chief Executive Officer is authorized to ensure that the information within this Policy is applied and that all actions comply with relevant legislation, policies, collective agreements, and terms and conditions of employment.

Obligations and Amendments:
The Library reserves the right to alter and amend this Policy as needed.