THE CORPORATION OF THE TOWNSHIP OF SOUTH STORMONT

BY-LAW No. 2025-049

BEING a by-law to amend By-law No. 2022-073, being a by-law to adopt an Electronic Monitoring Policy and to Adopt a Video Surveillance Policy.

WHEREAS the *Municipal Act, 2001*, c. 25 s. 5 (1) provides that the powers of a municipal corporation are to be exercised by its council;

AND WHEREAS the *Municipal Act, 2001*, c. 25 s. 5 (3) provides that the powers of every council are to be exercised by by-law;

AND WHEREAS Council did, on the 21st day of September, 2022, adopt By-law No. 2022-073, to adopt an Electronic Monitoring Policy;

AND WHEREAS Council deems it advisable to adopt a revised Electronic Monitoring Policy;

AND WHEREAS Council deems it advisable to adopt comprehensive Video Surveillance Policy.

NOW THEREFORE Council of the Corporation of the Township of South Stormont enacts as follows:

1. That By-law No. 2022-073 is hereby amended as follows:

   i. That Schedule "A" Electronic Monitoring Policy dated September 21, 2022 be deleted in its entirety and replaced with Schedule "A", being a revised Electronic Monitoring Policy, effective August 13, 2025, attached hereto and forming part of this by-law.

2. That all other relevant sections of By-law No. 2022-073 shall remain.

3. That the Video Surveillance Policy attached hereto as Schedule "B" and forming part of this by-law, be adopted.

4. That any other by-law inconsistent with this by-law is hereby repealed.

READ AND PASSED in open Council, signed and sealed this 13th day of August, 2025.

Mayor

Clerk

	TOWNSHIP OF SOUTH STORMONT
	Title: Electronic Monitoring Policy, Schedule "A" to By-law No. 2025-049 Schedule "A" to By-law No. 2022-073
	Policy Category: Human Resources Policies
	Effective Date: September 21, 2022
	Revision Date: August 13, 2025

Policy Statement

This Electronic Monitoring Policy has been implemented to inform employees that the Township of South Stormont **"the Township"** electronically monitors employees and to describe how and in which circumstances employees are electronically monitored and the purpose for which the information obtained through electronic monitoring may be used.

Purpose

The Township is committed to maintaining a transparent and fair workplace. Through this policy, the Township will address the manners in which it may monitor employees electronically, and the purposes for doing so. All uses of Township IT equipment and systems must abide by the Township's IT Acceptable Use Policy.

Scope

This policy applies to all Township of South Stormont employees of all work locations.

Policy

Monitoring employee usage of the Township's information technology assets (IT assets) is an essential part of enforcing Township policies, maintaining a respectful work environment, and ensuring that IT assets that are owned and managed by the Township are used safely and appropriately.

Building Systems

Building access system records the date and time each time a key fob is used whether access is granted or not. This information is used for auditing and security purposes. Building security systems record the date and time the security system is armed and disarmed. The system also records when a user enters their personal PIN code in the building security system to arm or disarm the building. This information may be used for auditing and improving security.

Computer Monitoring

The Township engages in Computer Monitoring to ensure that Township-owned IT resources are used in accordance with the Township's Acceptable Use Policy, and other Township policies where relevant.

Computer activity data may also be used to evaluate employee performance, detect malicious or high-risk activities, monitor network performance, and prevent security incidents from occurring.

Internet Monitoring

Internet use is logged while accessing the internet and is identifiable by device and user. The information is used to maintain security of our networks and auditing.

Employee Computer Monitoring Software

The Township's computer systems are monitored and managed with security and computer monitoring software provided by Optimus Tech Solutions. They could have access to employee computer activity data for the purpose of troubleshooting the software. Information accessed by Optimus Tech Solutions could be turned over to the Township for employment related purposes.

Email Monitoring

All email communications that are sent through Township-owned networks, equipment, or user accounts are subject to monitoring. The Township reserves the right to inspect email communication sent or received by Township employees if doing so is deemed necessary to maintain the security, confidentiality, and integrity of the Township, its systems, and the data that is in the Township's custody.

Personal Electronic Equipment

For employees who are permitted to use personal electronic equipment for work purposes ("Bring Your Own Device" or "BYOD"), the Township will make every reasonable effort to not electronically monitor the activities that take place on that device.

Employees participating in the BYOD program may have their personal electronic equipment, including computers, smart phones and tablet devices, monitored whenever accessing the Township's IT infrastructure, cloud-based applications, and any other IT assets. For example, Computer Monitoring will occur when personal electronic equipment is used on Township-owned wireless networks, virtual private

networks ("VPN"), and any other interaction from personal electronic equipment with Township-owned IT systems.

The Township reserves the right to inspect personal devices that are used by employees for work purposes if doing so is deemed necessary to maintain the security, confidentiality, and integrity of the Township, its systems, and the data that is in the Township's custody.

The Township reserves the right to remotely wipe all Township-owned data from personal electronic equipment. This will most commonly occur when a BYOD-eligible employee is no longer employed by the Township or personal electronic equipment is lost or stolen. For more information, please refer to the Township's Mobile Device Policy.

Vehicle Operation Monitoring

The Township may monitor employee's activity while operating a Township-owned vehicle The Township will maintain its vehicles, verify GPS tracking device reports to reduce the risk of injury to employees and the traveling public, improve efficiencies and minimize losses resulting from property damage claims.

Township vehicles are equipped with a Global Positioning System (GPS) which monitors vehicle operations including, but not limited to speed, location, seatbelt violation, aggressive driving, possible collision, plow/spreader operation metrics, idle times and routes. Monitoring such usage permits the Township to identify means by which to reduce fuel costs, increase driver safety, improve utilization efficiencies, and identify vehicle misuse. This information is also collected to meet regulatory compliance, addressing public complaints and auditing.

Additionally, Township Directors and/or Supervisors may regularly review GPS data to determine whether employees are operating Township vehicles safely within reasonable proximity of assigned work locations, efficient travel routes are being utilized, work activities are being planned efficiently, and reported activities correspond with designated work hours and assigned duties. Operation of a particular vehicle may be assessed at any time for business reasons.

When GPS monitoring reveals that an employee may have engaged in conduct violative of this policy or acceptable business practices, the Township shall evaluate all relevant information, including input from the employee. In determining whether corrective action is warranted, consideration shall be given to the nature, severity, and frequency of the violation(s).

Employees are strictly prohibited from any attempt to remove, disable or otherwise tamper with a GPS device installed on any Township vehicle.

Fuel Dispensing System

Fuel dispensing system records the date, time, fuel type, quantity, vehicle and user when fuel is dispensed. This information is used for allocating fuel costs and auditing.

Definitions

"Computer Monitoring" refers to the practice of collecting and/or accessing and reviewing user activity data on Township-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.

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

Monitoring and Compliance

In the event of a conflict or difference, the applicable provincial legislation supersedes this Policy.

This Policy supersedes other Township or divisional policies, standards and guidelines that govern the monitoring of IT assets to the extent of any conflict, subject to the principle that specific provisions of the other policies, standards, and guidelines continue to apply despite a more general provision being set out in this Policy.

The Township reserves the right to amend this Policy at any time.

Authority and Related Policies

Legislated Requirements:	*Employment Standards Act, 2000* *Working for Workers Act, 2022, Bill 88*
Related Policies:	Acceptable uses of IT Resources Policy

Contact

For more information on this policy, contact: Chief Administrative Officer.

	TOWNSHIP OF SOUTH STORMONT
	Title: Video Surveillance Policy Schedule "B" to By-law No. 2025-049
	Policy Category: All Departments
	Effective Date: August 13, 2025
	Revision Date:

Policy Statement

The Township of South Stormont is committed to:

- Community safety and crime prevention to promote a safe and desirable environment for residents, visitors and businesses.
- Balancing an individual's right to privacy, with the need to protect the safety and security of the public.
- Using best practices associated with responsible use of technology, including Video Surveillance Systems within Township of South Stormont Public Spaces and rights of ways.

Purpose

The purpose of this policy is to define criteria and processes associated with the installation and use of video surveillance equipment by the Township. Video surveillance shall be used to promote and foster a safe and secure environment for residents and staff, to ensure public safety for community members who visit or use Township Public Spaces, and to mitigate the risk of personal and municipal loss, theft or destruction of property.

Scope

This policy applies to Video Surveillance Systems located in Municipal Facilities and Public Spaces.

This policy does not apply to videotaping or audio taping of Council or Committee meetings, events or any covert surveillance that may be undertaken for the purposes of law enforcement. Further, this policy does not apply to the online streaming service governed under an independent agreement, provided by a third party, for streaming of sports related events in Township approved Municipal Facilities and / or Public Spaces.

Definitions

"MFIPPA"
Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56, as amended.

"Municipal Facilities"
Any building that is either owned or occupied by the Township and includes facilities leased by the Township.

"Personal Information"
Defined in Section 2 of MFIPPA, as recorded information about an identifiable individual, which includes, but is not limited to, information relating to an individual's race, colour, national or ethnic origin, sex and age. If a Video Surveillance System displays these characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered "personal information" under MFIPPA.

"Record"
Information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a videotape, a machine-readable record, and any record that is capable of being produced from a machine-readable record.

"Public Space"
Any area frequented by the general public that is owned, maintained, operated or occupied by the Township, including, but not limited to, parks, road allowanced, tunnels, boulevards, streets, courtyards, squares and bridges, sports venues, natural pathways, trails, as well as building exteriors, and significant interior public areas of municipal buildings.

"Township"
Corporation of the Township of South Stormont

"Video Surveillance System"
A video, physical or other mechanical electronic or digital surveillance system or device that enables continuous or periodic video recording, observing or monitoring of personal information about individuals.

Legislative Requirements

This policy reflects the provisions of MFIPPA.

The Municipal collection, storage of, and access to information recorded from video surveillance shall conform to published guidelines and practices as may be provided by the Information and Privacy Commissioner of Ontario (IPC) from time to time.

Personal Information collected by Township Video Surveillance Systems is done so under the authority of MFIPPA and will be used to ensure public safety and to mitigate the risk of personal and municipal loss or destruction of property.

Designated Responsibilities

a) The Chief Administrative Officer (CAO) will:
- Provide oversight and compliance with this policy by all Township employees.

b) Corporate Services will:

- Respond to requests for disclosure under the Freedom of Information or applicable or routine disclosure procedures;
- Ensure a public notice for video surveillance is placed at all Township sites that have a Video Surveillance System;
- Respond to requests from the public and employees about the collection, use, and disclosure of personal information captured by a Video Surveillance System;
- Respond to appeals and privacy complaints received through the Office of the Information and Privacy Commissioner of Ontario (IPC);
- Educate employees and visitors on the collection, use, and disclosure of personal information through the Video Surveillance System;
- Work with department manager(s) and employee(s) in the event of an improper disclosure of personal information;
- Notify the IPC in the event of a privacy breech, where appropriate;
- With the support of Recreation and Facilities, conduct internal audits of the system as required to ensure compliance with this policy and MFIPPA.

c) Recreation and Facilities shall:

- Authorize installation of security cameras and surveillance practices;
- Assist Corporate Services as required in the processing of applications for access to information submitted by individuals under MFIPPA;
- Recommend the placement of each security camera based upon documented, justifiable grounds for each;
- With the support of Corporate Services, develop and provide training regarding awareness and compliance with MFIPPA, including employee responsibilities and how to handle information inquiries.

d) Directors and Managers will:

- Ensure the appropriate use of the Video Surveillance System at their Municipal Facilities and Public Spaces in compliance with this policy;
- Delegate and assign responsibility regarding who will act on their behalf in following procedures relating to this policy in their absence;
- Provide job specific training;
- Refer any requests for copies of surveillance video to Corporate Services;
- Report any privacy breeches to Corporate Services;
- Ensure that employees are monitoring compliance with the retention periods applicable to the Video Surveillance Systems.

e) Employees will

- Report any suspected privacy breach to their Manager;
- Report any problems with the Video Surveillance System to their Manager;
- Review and comply with this policy and MFIPPA in performing their duties and functions related to the operation of the Video Surveillance System.

Human Asset Management

Video Surveillance Systems are used on Township premises to ensure that employees and patrons are kept secure from forms of misconduct. Should unlawful activity be discovered or activity that is or may be considered a breach of Township policy and standards, the recordings captured by the Video Surveillance System will be used to address those circumstances, including the possibility of disclosure to authorized third parties.

Video Surveillance Systems will not be used in areas where employees have a reasonable expectation of privacy, such as bathrooms and changing rooms. Where Video Surveillance Systems are used, the equipment will be made clearly visible and there will be notices indicating the presence of the equipment.

Employees may be subject to criminal charges, civil liability and/or discipline, including but not limited to termination, for a breach of this policy, or provisions of MFIPPA or other relevant statutes.

Signage and Notification

A notice of collection will be posted on the Township website and shall state the following:

a) The legal authority for the collection;

b) The principal purpose or purposes for which the personal information is intended to be used; and

c) The title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

Signage will be prominently displayed at the perimeter of the monitored areas and at key locations within these areas. Signage shall include basic information to notify the public and staff of the Township use of video surveillance in the area.
Examples of signage and the website's notice of collection are attached as Appendix A.

Operation and Access

a) Video Surveillance Systems shall be operated by authorized personnel only.

b) Video surveillance footage will not be used to monitor patrons' general use of Municipal Facilities or Public Spaces. Circumstances which warrant review will be limited to security concerns that have been reported, or in the investigation of an incident or potential crime.

c) Designated staff will have the authority to monitor real time camera feeds and review records of images and/or authorize the release from the system for investigation or other purposes. These designated staff include:

- CAO
- Director of Corporate Services/Clerk;
- Director of Recreation and Facilities; and
- Additional staff as required and delegated in writing, by one of the above.

d) Authorized personnel may only view or make record of video when directed to do so by designated staff as a direct result of:
   - a request made by law enforcement;
   - under MFIPPA; or
   - an internal Public Space or Municipal Facilities related incident.

e) All requests for access to, and release of video surveillance Records, shall be subject to MFIPPA and shall be directed to Corporate Services. Corporate Services, in cooperation with the Manager of Facilities shall process MFIPPA requests, in accordance with the legislation.

f) Records required for the purpose of law enforcement require the requestor to complete the Law Enforcement Access Request Form (Attached as Appendix B) and forward it to the Director of Corporate Services/Clerk. The Director of Corporate Services/Clerk will then provide the Record, via secure SharePoint site, for the specified date and time of the incident to their requestor subject to compliance with MFIPPA. At minimum the following information will be collected:
   - Name of requestor;
   - Investigation number and reason for the request;
   - The date and time of the original, recorded incident including the designated name/number of the applicable camera;
   - Date and time the Record was securely provided to the requestor.

Records and Retention

a) Records may be disclosed in responding to the following incidents:
   - Destruction and vandalism of property
   - Activities involved in breach of physical security or data / cyber security
   - Public safety, including harassment
   - Required for the purposes of law enforcement

b) Records will be retained for 14 days from the date of use, after which, the Records will be cleared or overwritten within the Video Surveillance System.

c) Records containing Personal Information that will be retained in excess of 30 days may include:
   - Personal Information that has been viewed for law enforcement and public safety purposes which must be retained for a certain period thereafter.
   - Personal Information that is associated with an internal investigation. Such material will be maintained until the investigation has been resolved.

- Personal Information that is associated with a Freedom of Information request under MFIPPA. Such material will be stored pursuant to the Township's approved Records Retention schedule.

Unauthorized Disclosure

In the event of a collection, use, disclosure or retention in violation of applicable privacy laws, the Township will comply with the recommendations of the Office of Information and Privacy Commissioner of Ontario in responding to breaches. The Clerk will respond to any inadvertent disclosure of Personal Information.

Policy Review

This policy will be reviewed once every four (4) years, or as necessary.

Contact

For more information on this policy, contact:

Director of Corporate Services/Clerk
Township of South Stormont
P.O. Box 84, 2 Mille Roches Road
Long Sault, ON K0C 1P0
613-534-8889, Ext.