THE CORPORATION OF THE TOWNSHIP OF SOUTH STORMONT

BY-LAW NO. 2022-073

<u>BEING</u>   a by-law to adopt an Electronic Monitoring Policy.

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

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

<u>AND WHEREAS</u>   Council deems it advisable to adopt an Electronic Monitoring Policy for the Township of South Stormont.

<u>NOW THEREFORE</u>   Council of the Township of South Stormont enacts as follows:

    1.   That the Electronic Monitoring Policy attached hereto as Schedule "A" and forming part of this by-law, be adopted.

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   That any other by-law inconsistent with this by-law is hereby repealed.

READ AND PASSED in open Council signed and sealed this 21st day of September, 2022.

_____
Mayor

_____
Clerk

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

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.

Video Surveillance

Video surveillance equipment is used on Township premises to ensure that employees, patrons, and Township-owned assets are kept secure from theft, vandalism, and other 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 video surveillance equipment will be used to address those circumstances—including the possibility of disclosure to authorized third parties.

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

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.