



# St. Thomas Police Service

## BOARD POLICY

Subject:	Electronic Monitoring of Employees
Policy Number:	AI – 029 – Electronic Monitoring of Employees
Effective Date:	April 1, 2024
Reviewed:	April 22, 2026
Authorized:	Police Services Board

### AUTHORITY/LEGISLATIVE REFERENCE

- *Community Safety and Policing Act, 2019*
- *Employment Standards Act, 2000, S.O. 2000, c.41*

### POLICY STATEMENT

The St. Thomas Police Service Board (the “Board”) is committed to transparency regarding the electronic monitoring of employees. The purpose of this policy is to ensure that any electronic monitoring conducted by the St. Thomas Police Service (the “Service”) is carried out in a manner that is consistent with legislative requirements, respects privacy considerations, and supports legitimate operational and administrative objectives.

### POLICY APPLICATION

1. The Service may implement electronic monitoring of employees where necessary for legitimate operational, safety, security, administrative, or investigative purposes.
2. Electronic monitoring may include, but is not limited to, the monitoring of email usage, internet activity, telephone usage, location data, body-worn cameras, in-car cameras, access control systems, and other digital systems used in the course of employment.
3. The Chief of Police shall establish procedures governing the use of electronic monitoring, including the circumstances in which monitoring may occur, the type of information collected, and the purposes for which it may be used, and shall ensure that any disclosure of personal information obtained through electronic monitoring is consistent with applicable Service policies, including HR-26 Electronic Monitoring Policy and Directive.
4. Employees shall be informed of the existence of electronic monitoring practices, including the types of monitoring that may occur and the purposes for which information may be used, in accordance with legislative requirements.
5. Information obtained through electronic monitoring shall be used only for legitimate purposes and handled in accordance with applicable privacy, records management, and confidentiality

requirements.

6. Nothing in this policy creates an expectation of privacy for employees when using Service-owned equipment, systems, or networks, subject to applicable legislation.
7. The Board shall review this policy periodically to ensure ongoing compliance with legislative requirements and best practices.