SECTION:	NUMBER:
AD	4

SUBJECT: VIDEO SURVEILLANCE POLICY

1.0 PURPOSE

1.1 It is the policy of the Municipality to utilize Video Surveillance Systems to increase the safety and security of individuals, assets and property and to detect and deter criminal activity and vandalism. In the event of a reported or observed incident, the review of recorded information may be used to assist in the investigation of the incident.

1.2 The Municipality recognizes that video surveillance technology has a potential for infringing upon an individual's right to privacy and although a Video Surveillance System may be required for legitimate operational purposes, its use must be in accordance with the provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*).

1.3 This policy will provide guidelines to assist Municipal Departments that have identified an appropriate use for Video Surveillance Systems, and to manage records that may be created using this technology in a manner that complies with *MFIPPA* and record management requirements.

2.0 LEGISLATIVE AUTHORITY

2.1 Section 11(1) of the *Municipal Act, 2001,* S.O. 2001, c. 25, as amended, provides that a lower-tier municipality may provide any service or thing that the municipality considers necessary or desirable for the public.

3.0 SCOPE

3.1 This policy applies to all areas within the jurisdiction of the Municipality.

3.2 This policy does not apply to videotaping or audio recording of Municipal Council or Committee meetings.

4.0 DEFINITIONS

"CAO" – shall mean the Chief Administrative Officer (CAO) or designate duly appointed by the Municipality as prescribed in Section 229 of the *Municipal Act, 2001*, S.O. 2001, c. 25, as amended.

"Clerk" – shall mean the Clerk or designate duly appointed by the Municipality as prescribed in Section 228 of the *Municipal Act, 2001*, S.O. 2001, c. 25, as amended.

"Employee" – all union and non-union employees of the Municipality.

"Municipal Department" – shall mean the department that runs a particular service area of the Municipality.

"Personal Information" – is defined in Section 2 of the *Municipal Freedom of Information and Protection of Privacy Act ("MFIPPA")*, as recorded information about an identifiable individual, which includes, but is not limited to, information relating to an individual's race, national or ethnic origin, colour, age or sex. 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".

"Senior Managers" – shall mean the Senior Managers who lead or supervise a particular service area of the Municipality.

"Service Providers" – shall mean a consultant or other contractor engaged by the Municipality in respect of the Video Surveillance System or Equipment.

"Storage Device" – refers to a videotape, computer disk or drive, CD ROM, computer chip or other device used to store the recorded data or visual, audio or other images captured by a Video Surveillance System.

"Municipality" – shall mean the Corporation of Tay Valley Township.

"Video Surveillance Equipment" – shall mean the equipment or device used to receive or record the Video Surveillance Record collected though a Video Surveillance System, including a camera or video monitor or any other video, audio, physical or other mechanical, electronic or digital device.

"Video Surveillance Record" – shall mean any record of 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.

"Video Surveillance System" – shall mean 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 in open, public spaces.

5.0 POLICY REQUIREMENTS

5.1 Prior to Installation

5.1.1 Prior to installation of a Video Surveillance System, the Municipality shall consider the following:

- the use of a Video Surveillance System should be based on verifiable, specific incidents of crime or significant safety concerns, protection of municipal property or for crime prevention ;
- an assessment of the situation has determined that less intrusive means of achieving the same goals have been considered or attempted and are substantially less effective than video surveillance or are not feasible; and
- the benefits of video surveillance substantially outweigh the reduction of privacy inherent in the use of video surveillance.

5.1.2 Prior to installation of a Video Surveillance System, the Municipality shall ensure that any agreements between the Municipality and its Service Providers state that the Records dealt with or created while creating a Video Surveillance Record are under the Municipality's custody and are subject to privacy legislation (MFIPPA).

5.2 Location and Operation

5.2.1 The Municipality shall install Video Surveillance Equipment in identified public areas only where video surveillance has been determined necessary in accordance with this policy.

5.2.2 The Municipality shall not install Video Surveillance Equipment inside areas where individuals have a higher expectation of privacy such as change rooms, washrooms or other similar areas where personal privacy and/or confidentiality is expected.

5.2.3 The Municipality may install visible and/or hidden Video Surveillance Equipment; however signage notifying the public of the existence of Video Surveillance Equipment shall be present in all situations.

5.2.4 Video Surveillance Equipment shall be installed in such a way that it only monitors those areas that have been identified as requiring video surveillance.

5.2.5 A Video Surveillance System may operate at any time within a 24-hour period.

5.2.6 While Video Surveillance Equipment may be continuously recording, they may be only periodically monitored.

5.3 Notification

5.3.1 The public shall be notified of the existence of Video Surveillance Equipment by clearly written signs prominently displayed at the entrances, exterior walls, and interior of buildings and/or the perimeter of the video surveillance areas.

5.3.2 Signage shall satisfy the notification requirements under Section 29 (2) of *MFIPPA*, as amended, which includes informing individuals of:

- the legal authority for the collection of Personal Information;
- the principal purpose(s) for which the Personal Information is intended to be used; and
- the title, business address and telephone number of a Senior Manager of the Municipality who can answer questions about the collection.

5.4 Access, Use and Disclosure

5.4.1 A Video Surveillance Record shall only be accessed in the event of a reported, observed or suspected incident that affects the safety and security of individuals, assets and property of the Municipality. The review of recorded information may be used to assist in the investigation of the incident.

5.4.2 Only the Chief Administrative Officer, Senior Managers and Service Providers shall have access to the Video Surveillance Equipment and have the ability to review a Video Surveillance Record.

5.4.3 Logs shall be kept of all instances of access to, use of, maintenance and storage of a Video Surveillance Record to enable a proper audit trail.

5.4.4 All logbook entries shall detail the Senior Manager, date, time and activity when accessing any Video Surveillance Record.

5.4.5 All Storage Devices that are not in use shall be dated, labeled and securely stored.

5.4.6 All public requests for Video Surveillance Records shall be directed to the Clerk in writing either in the form of a letter or on the prescribed Request for Access to Information form under *MFIPPA,* as amended.

5.4.7 Video Surveillance Records may also be disclosed to a law enforcement agency as outlined in Section 32 (e) and 32 (g) of *MFIPPA,* as amended.

5.5 Retention Period of Video Surveillance Records

5.5.1 Video Surveillance Equipment shall be programmed with a maximum retention period of five (5) calendar days after which time it is overwritten.

5.5.2 If a Video Surveillance Record is proactively pulled in anticipation of a request, the Video Surveillance Record may be stored for up thirty (30) calendar days. If no request is received within the thirty (30) days then it shall be manually deleted.

5.5.3 A Video Surveillance Record which has been requested shall be retained until the investigation has resolved or as required by law.

5.5.4 Video Surveillance Equipment shall only be destroyed when replaced by a new piece of Video Surveillance Equipment or when it is not repairable.

5.5.5 Video Surveillance Equipment shall only be destroyed by an authorized Service Provider and destroyed in a manner that ensures that the Video Surveillance Equipment can no longer be used by any person and that the information recorded cannot be reconstructed or retrieved by any person.

6.0 PRIVACY BREACH

6.1 The Municipality shall take immediate action upon learning of a privacy breach, including, but not limited to:

- notifying all relevant Employees of the breach, including the delegated Head under MFIPPA;
- notifying the Information and Privacy Commissioner of Ontario;
- identifying the scope of the breach and taking the necessary steps to contain it;
- notifying those individuals whose privacy was breached; and
- conducting an investigation.

6.2 A breach of this Policy by Employees may result in disciplinary action.

6.3 A breach of this Policy by a Service Provider may result in the cancellation of the Municipality's contract with that Service Provider.

7.0 TRAINING

7.1 The Chief Administrative Officer, Senior Managers and Service Providers shall be trained in the use of the Video Surveillance Equipment and this Policy.

7.2 The Chief Administrative Officer, Senior Managers and Service Providers shall sign a confidentiality agreement regarding their duties under this Policy and the MFIPPA.

8.0 AUDITS

8.1 The Municipality's Video Surveillance System and Policy shall be reviewed every two (2) years to ensure that:

- video surveillance continues to be justified, and if so, whether its use should be restricted;
- access to, use of, maintenance and storage of Video Surveillance Records are properly recorded in the logbooks;
- retention policies for Video Surveillance Records are being followed; and
- requests for Video Surveillance Records have been tracked.

8.2 Any deficiencies or concerns identified shall be addressed as soon as practicable.

9.0 ACCOUNTABILITY FRAMEWORK

9.1 The Chief Administrative Officer and Senior Managers are responsible for ensuring compliance with this policy.

10.0 POLICY REVIEW

This Policy shall be reviewed at least once every two (2) years or as required based on revisions to corporate practices or legislation.

11.0 REFERENCES

Other Resources

Frank Cowan Company: Risk Management Considerations for Video Surveillance
Information and Privacy Commissioner of Ontario: Guidelines for the Use of Video Surveillance
Information and Privacy Commissioner of Ontario: Privacy Breach Protocol & Guidelines for Government Organizations
Municipal Freedom of Information and Protection of Privacy Act