Municipality of Leamington
live | play | work

Policy No.: A00 –Video Surveillance Policy
Date Enacted: September 24, 2017
Amended By:

---

1. Subject

1.1 The Municipality of Leamington recognizes the need to balance an individual's right to privacy and the need to ensure the safety and security of municipal employees, clients, visitors and property. While video surveillance cameras are installed for safety and security reasons, the Municipality's video surveillance systems must also be designed to minimize privacy intrusion. Proper video surveillance, where deemed necessary, is one of the most effective means of helping to keep municipal facilities and properties operating in a safe, secure, and privacy protective manner.

2. Application

2.1 This policy applies to all types of camera surveillance systems, surveillance monitors and camera recording devices at municipally owned properties that are used for security purposes. This policy does not apply to video surveillance used for employment-related or labour-related information. This policy does not apply to the videotaping or the audiotaping of Council meetings.

3. Purpose

3.1 This policy has been developed to govern security video surveillance at municipally owned/operated/leased facilities in accordance with the provisions of the Municipal Freedom of Information and Protection of Privacy Act.

3.2 Video security surveillance systems, when used with other security measures, is an effective means of ensuring the security and safety of municipal facilities, the individuals who use them, and the assets housed within them. However, the need to ensure security and safety must be balanced with an individual's right to privacy. The purpose of this policy is to establish guidelines which are intended to achieve a balance between security and safety and an individual's right to privacy. Specifically, this policy addresses requirements and responsibilities with regard to:

- Installation of the video surveillance systems;
- Operation of the video surveillance systems;
- Use of the information obtained through the video surveillance systems ; and

- Custody, control and access to records created through the video surveillance systems.

4. Definitions

Act is defined as Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56.

Clerk is defined as the Clerk of the Corporation of The Municipality of Leamington.

Disclosure is defined as the release of relevant information which includes, but is not limited to, viewing a recording, as well as making a copy of a recording.

Facility is defined as any building or land that is either owned or occupied by the Corporation of the Municipality of Leamington.

Municipality is defined as the Corporation of The Municipality of Leamington.

Personal information is defined in Section 2 of the Act 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 the Act.

Reception Equipment refers to the equipment or device used to receive or record the personal information collected through a video surveillance system, including a camera or video monitor or any other video, audio, physical or other mechanical, electronic or digital device.

Record as defined in Section 2 of the Act, means 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.

Storage Device refers to a videotape, computer disk or drive, CD ROM, computer chip, digital recording, or other device used to store the recorded data or visual, audio or other images captured by a video surveillance system.

Video Surveillance System refers to a video, physical or other mechanical, electronic, digital or wireless surveillance system or device that enables continuous or periodic video recording, observing or monitoring of personal information about individuals in open, public spaces (including streets, highways, and parks).

5. Considerations

5.1 Prior to installation of video surveillance equipment, the Municipality must consider the following:

(a) The use of video surveillance should be considered in relation to an articulable concern for the safety of individuals or the protection of property.

(b) Video cameras should only be installed in identified public areas where video surveillance is a necessary and viable detection or deterrence activity.

(c) An assessment of the privacy implications should be conducted of the effects that the proposed video surveillance system may have on personal privacy, and the ways in which any adverse effects may be mitigated by examining collection, use, disclosure, and retention of personal information.

(d) A requirement that any agreements between the Municipality and service providers stating that the records dealt with or created while delivering a video surveillance program are under the Municipality's control and subject to privacy legislation (MFIPPA).

(e) A requirement that employees and service providers (in the written agreement) review and comply with the policy and the Act in performing their duties and functions related to the operation of the video surveillance system

6. Installation and Placement

6.1 Video surveillance equipment should never monitor the inside of areas where the public has a higher expectation of privacy such as change rooms and washrooms.

6.2 Equipment should be installed in a strictly controlled access area. Only controlling personnel should have access to the access area and the equipment.

6.3 Equipment should be installed in such a way that it only monitors those spaces that have been identified as requiring video surveillance.

6.4 Adjustment of the camera position should be restricted, if possible, to ensure only designated areas are being monitored.

7. Notification

7.1 The public should 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 perimeter of the video surveillance areas.

7.2 Signage must satisfy the notification requirements under Section 29(2) of the Act, which include: 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 someone who can answer questions about the collection.

7.3 The following is suggested wording for use in building signage, based on a minimum requirement of the Information and Privacy Commission:

"This area is monitored by video surveillance cameras. The personal information collected by the use of the camera at this site is collected under the authority of the (insert authority of Act or By-law). This information is used for the purpose of promoting public safety and protection of property at this site. Please direct inquiries to: (title, business address and phone number of someone who can be contacted during business hours to answer questions about the collection of personal information)."

8. Operation of Video Surveillance Systems

8.1 The Manager of Information Technology (the “Manager”) is authorized to designate persons to operate the video surveillance system.

8.2 The Manager will maintain a list of all persons designated and only those who have been designated can operate the systems.

8.3 The Manager is responsible for establishing an appropriate training program for the operation of the equipment, including operator responsibilities with respect to protection of privacy and confidentiality, and for ensuring that all system operators are trained appropriately.

9.0 Use of Information Collected

9.1 The information collected through video surveillance is used only:

- To investigate an incident involving the safety or security of people, facilities, or assets;
- To provide law enforcement agencies with evidence related to an incident under police investigation;
- To provide evidence as required to protect the Municipality's legal rights;
- To respond to a request for information under the Municipal Freedom of Information and Protection of Privacy Act;
- To investigate an incident or allegation of serious employee misconduct; or
- To investigate an incident involving an insurance claim.

10. Retention Period of Information

10.1 The retention period for information that has not been viewed for law enforcement or public safety purposes shall be 14 days. Recorded information that has not been viewed will be routinely erased.

10.2 Information that has been viewed by municipal staff but does not appear to present any information pertinent to the protection of corporate assets or the safety of the public and employees, will be automatically erased through the re-write process.

10.3 When recorded information has been viewed for law enforcement or public safety purposes, the retention period shall be a minimum of one (1) year from the date of viewing unless involved in an active police investigation.

10.4 The Municipality will store and retain storage devices required for evidentiary purposes according to standard procedures until the law enforcement authorities request them.

11. Storage

11.1 All tapes or other storage devices that are not in use should be dated, labeled and stored securely in a locked container located in a controlled access area.

12. Requests for Access by the Public

12.1 In accordance with the act, any person may make a written request to the Clerk for access to digital records obtained through the use of the surveillance system by completing the Municipality's Application for Access or Correction to Records form and by submitting the non-refundable mandatory application fee.

12.2 The Clerk will review the legal authority of such person to receive the requested information, as indicated under the Act.

12.3 When access to a record is given, the following information will be included in the Clerk's access log book for audit purposes:

- Date and time access was allowed or the date on which disclosure was made;
- Identification of the party allowed access or to whom disclosure was made;
- Reason for allowing access or disclosure;
- Extent of the information to which access was allowed or which was disclosed; and
- Provisions for the return of the record or its destruction.

12.4 When a request is made for a video record it shall be removed from the rotational cycle. The removed video record shall be clearly marked to indicate its removal and secured in such a way that it cannot be recorded over. It shall remain securely stored until the police arrive to review and/or take custody of the videotape. In the event that a video record is in digital form, a separate file may be created and transferred to the Police in a secure format.

12.5 The Clerk will provide direction to staff to provide this information or part thereof in accordance with the Act.

12.6 Access to personal information may depend on whether there is an unjustified invasion of another individual's privacy and whether any exempt information can reasonably be severed from the record.

12.7 The Clerk may charge fees for this service in accordance with MFIPPA.

13. Requests for Access by a Law Enforcement

13.1 If access to a video surveillance record is required for the purpose of law enforcement investigation, the requesting officer must complete the "Law Enforcement Officer Request" form and forward it to the Clerk.

13.2 The Clerk will review the requests on a case-by-case basis to determine whether disclosure will be granted. Depending on the nature of the request, law enforcement may be required to complete a formal Freedom of Information request.

13.3 When access to a record is given, the following information will be included in the Clerk's access log book for audit purposes:

- Date and time access was allowed or the date on which disclosure was made;
- Identification of the party allowed access or to whom disclosure was made;
- Reason for allowing access or disclosure;
- Extent of the information to which access was allowed or which was disclosed; and
- Provisions for the return of the record or its destruction.

13.4 When a request is made for a video record it shall be removed from the rotational cycle. The removed video record shall be clearly marked to indicate its removal and secured in such a way that it cannot be recorded over. It shall remain securely stored until the police arrive to review and/or take custody of the videotape. In the event that a video record is in digital form, a separate file may be created and transferred to the Police in a secure format.

Responsibilities

14.1 The Manager of Information Technology is responsible for the overall corporate video surveillance program and the management of authorized video security systems, including assisting other managers with specifications, equipment standards and installation.

14.2 The Manager of Information Systems or designated staff, is responsible for assisting with evaluation of video surveillance equipment to be procured and installation and operation of equipment, making a copy of a record in approved circumstances and overseeing the disposal of any storage device.

14.3 The Clerk will respond to requests for access to video surveillance records from the public and law enforcement agencies, respond to appeals and privacy complaints through the Office of the Information and Privacy Commissioner of Ontario, notify the Information and Privacy Commissioner of Ontario in the event of a privacy breach where appropriate and charge fees for the production of records in accordance with MFIPPA. The Clerk will also document all information regarding the use, maintenance and storage of records in the applicable logbook, including all instances of access to, and use of, recorded material to create a proper audit trail.

Unauthorized Disclosure/Access

15.1 Any Municipality of Leamington employee having knowledge of an unauthorized disclosure of a record or unauthorized access must immediately inform the Clerk of the breach. The Clerk will inform the Director of Legal and Legislative Services, and together they will take all reasonable actions to recover the record and limit the record's exposure.

16. Contact

16.1 For more information related to video surveillance systems, contact the Clerk or Director of Legal and Legislative Services.