Security Video Surveillance Policy

Policy Statement

The Municipality of Central Elgin (the Municipality) 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.

As an institution governed by the *Municipal Freedom of Information and Protection of Privacy Act R.S.O. 1990, Chapter M. 56*, the Municipality of Central Elgin has obligations with respect to notice, access, use, disclosure, retention and disposal of records.

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 way that protects security, safety, and privacy. Personal information collected by video surveillance includes video images and audio.

Policy Description

This Municipal policy has been developed to govern video surveillance at municipally owned and leased properties in accordance with the privacy provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

The Municipal Freedom of Information and Protection of Privacy Act

As detailed in Section 38(2) of Freedom of Information and Protection of Privacy Act (FIPPA) and 28(2) of Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), personal information may be collected without consent when it is:

1. expressly authorized by statute or by-law,
2. used for the purposes of law enforcement, or
3. necessary to the proper administration of a lawfully authorized activity.

This policy has been drafted to conform with practices outlined by the Information and Privacy Commissioner of Ontario ("IPC") in a document entitled "Video Surveillance: The Privacy Implications", available at https://www.ipc.on.ca/wp-content/uploads/Resources/2015_Guidelines_Surveillance.pdf. The IPC has indicated that after careful consideration, an institution may decide to use video surveillance for purposes in accordance with MFIPPA. Section 2 of MFIPPA defines "videotapes" in the term "record" and also provides a definition of "personal information" which describes it as recorded information about an identifiable individual.

Application

This policy applies to all types of camera surveillance systems, surveillance monitors, and camera recording devices at municipally owned and leased properties that are used for security purposes.

This policy does not apply to Agencies, Boards, and Commissions; or to cameras used by the Ontario Provincial Police; or, to video surveillance used for employment related or labour-related information; or, to cameras used for the reduction of liability for the surveillance of roads and their conditions.

Responsibilities

The senior staff member responsible for the Video Surveillance Policy is the Director of Physical Services or his or her assignees. The Director of Physical Services may delegate responsibilities under this Policy to other staff.

The Chief Administrative Officer/Clerk is Municipality's Head under the Municipal Freedom of Information and Protection of Privacy Act ("MFIPPA"), and is responsible for providing a response to access requests.

The key duties of the Director of Physical Services include:

- Ensuring policy compliance.
- Undertaking yearly evaluations of video surveillance system installations to ensure compliance with this Policy.
- Approving installation of video cameras at specified municipally owned and leased properties.
- Advising on placement of video surveillance monitoring signs.
- Acting as the primary contact for all requests by law enforcement agencies for access to video records.
- Overseeing day-to-day operations of video surveillance cameras.
- Complying and ensuring Operator's compliance with all aspects of the Security Video Surveillance Policy.
- Ensuring monitoring and recording devices are stored in a safe and secure location.
- Ensuring logbooks, recording all activities related to video devices and records, are kept and maintained.
- In consultation with Human Resources, providing training on a regular basis regarding obligations and compliance with the MFIPPA and the Security Video Surveillance Policy.
- Ensuring that no copies of data/images in any format (hardcopy, electronic, etc.) is taken from the video surveillance system inappropriately
- Immediately reporting all alleged privacy breaches to the Chief Administrative Officer for immediate action.
- Working with the Chief Administrative Officer to investigate video surveillance security privacy breaches.

- Providing status updates to Council, annually, regarding staff adherence to the responsibilities within the policy.
- Reporting to Council when video surveillance is being proposed in new locations.
- Ensuring that they and their assignees receive appropriate training.

All Staff must adhere to the video surveillance policy and must not access or use information contained in the video surveillance system, it's components, files, or database for personal reasons, nor dispose, destroy, erase or alter any record without proper authorization and without following the regulations contained in the Security Video Surveillance Policy.

Guidelines to Follow Prior to the Installation of a Video Surveillance System

Before deciding to install video surveillance, the following factors must be considered:

- The use of video surveillance cameras should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns.
- A video surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable.
- An assessment must be conducted on the effects that the proposed video surveillance system may have on personal privacy, and the ways in which any adverse effects can be mitigated.
- The proposed design and operation of the video surveillance systems should minimize privacy intrusion.
- Whether or not additional sensory information, such as sound, is directly related to potential problems or does not need to be recorded.

When designing a video surveillance system and installing equipment, the following must be considered:

- The video surveillance systems may operate at any time in a 24 hour period.
- The video equipment should be installed to only monitor those spaces that have been identified as requiring video surveillance.
- The ability to adjust cameras should be restricted, if possible, so that the cameras do not record and operators cannot adjust or manipulate cameras to overlook spaces that are not intended to be covered by the video surveillance program, such as through windows in adjacent buildings or onto adjacent properties.
- Equipment should never monitor the inside of areas where the public and employees have a higher expectation of privacy (e.g. change rooms and washrooms). –
- Where possible, video surveillance should be restricting to periods when there is a demonstrably higher likelihood of crime being committed and detected in the area under surveillance.
- Viewing and recording equipment must be located in a strictly controlled access area.
- Only identified and trained staff shall have access to the controlled access area and the reception/recording equipment.
- Every reasonable attempt should be made to ensure video monitors are not in a position that enables the public and/or unauthorized staff to view the monitors.

Notice of Use of Video Systems

In order to provide notice to individuals that video is in use:

- The Municipality shall post signs, visible to members of the public, at all entrances and/or prominently displayed on the perimeter of the grounds under video surveillance (see Appendix #2).
- The notification requirements of this sign must inform individuals, using words and symbols, 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 (see Appendix #2).
- This information will also be available on the Municipal website.

Personnel Authorized to Operate Video Equipment

Only the Director of Physical Services, and staff designated by the Director, shall be permitted to operate video surveillance systems.

Video Equipment / Records

Types of Recording Devices
The Municipality may use Digital Video Recorders (DVR) in its video systems. Facilities using video recorders will retain these records for a period of up to 30 days, depending on the recording device and technology. A record of an incident will only be stored longer than 30 days where it may be required as part of a criminal, safety, or security investigation or for evidentiary purposes.

Monitors will be kept in a secure location where they are not visible to the public.

Record Identification
All records (storage devices) shall be clearly identified (labeled) as to the date and location of origin. They shall be labeled with a unique, sequential number or other verifiable symbol. In facilities with a DVR that stores information directly on a harddrive, the computer time and date stamp shall be understood to be this identification. In facilities with a VCR or other recording mechanism using a removable / portable storage device, the operator shall affix a label to each storage device identifying this information.

Logbook
Each device shall have a logbook to record all activities related to video devices and records. The activities include all information regarding the use, maintenance, and storage of records and all instances of access to, and use of, recorded material. All logbook entries will detail authorized staff, date, time, and activity. This logbook must remain in a safe and secure location

with the video recording equipment. Only the Director of Physical Services is authorized to remove this logbook from the secure location.

Access to Video Records

Access
Access to the video surveillance records, e.g. remote access using the internet, logbook entries, CD, video tapes, etc shall be restricted to authorized personnel only to in order to comply with their roles and responsibilities as outlined in the Video Surveillance Policy.

Any staff accessing records should sign a written agreement to adhere to this policy, including an undertaking of confidentiality.

Storage
All storage devices that are not in use must be stored securely in a locked receptacle located in an access-controlled area.

Formal Access Requests Process
With exception of requests by law enforcement agencies, all requests for video records should be directed to the main office at 450 Sunset Drive in St. Thomas, Ontario for processing.

A person requesting access to a record should make a request in writing either in the form of a letter or the prescribed form and submit it to the Chief Administrative Officer under MFIPPA. This form is available in our offices, or at www.centralelgin.org.

The individual requesting the record must:

- Provide sufficient detail (the approximate time and date, the location - if known - of the incident, etc.) to enable an experienced employee, upon a reasonable effort, to identify the record; and,
- At the time of making the request, pay the prescribed fees as provided for under the Act.

Access: Law Enforcement
If access to a video surveillance record is required for the purpose of a law enforcement investigation, the requesting Officer must complete the Law Enforcement Officer Request Form (See Appendix #1) and forward this form to the Director of Physical Services.

While there may be other situations where the disclosure of video surveillance footage is permitted, video surveillance may be disclosed to a law enforcement agency when:

- the law enforcement agency approaches the Municipality with a warrant requiring the disclosure of the footage, as per section 42(1)(e) of FIPPA and section 32(e) of MFIPPA,
- the law enforcement agency approaches the Municipality, without a warrant, and requests the disclosure of footage to aid an investigation from which a proceeding is likely to result, as per section 42(1)(g) of FIPPA and section 32(g) of MFIPPA, or

- staff observe an illegal activity on Municipality property and disclose the footage to a law enforcement agency to aid an investigation from which a proceeding is likely to result, as per section 42(1)(g) of FIPPA and section 32(g) of MFIPPA.

Staff will provide the recording for the specified date and time of the incident as requested by the Law Enforcement Officer and record the following information in the facility's video logbook:

i) the date and time of the original, recorded incident including the designated name/number of the applicable camera and DVR;
ii) the time and date the copy of the original record was sealed;
iii) the time and date the sealed record was provided to the requesting Officer;
iv) the case file number of the agency's investigation,
v) a description of the circumstances justifying the disclosure;
vi) the amount of footage involved;
vii) the name, title and agency to whom the footage is being disclosed;
viii) the legal authority for the disclosure,
ix) the means used to disclose the footage and
x) if the record will be returned or destroyed after use by the Law Enforcement Agency.

This must only be completed by an individual(s) authorized in a private, controlled area that is not accessible to other staff and/or visitors.

In order to protect privacy, the Municipality will, whenever possible, strongly encrypt video surveillance footage at rest and when transmitted across open, public networks, and store physical records of footage, such as discs, memory cards or servers, in a locked facility.

Custody, Control, Retention and Disposal of Video Records / Recordings

The Municipality retains custody and control of all original video records not provided to law enforcement.

Video records are subject to the access and privacy requirements of the MFIPPA, which includes but is not limited to the prohibition of all Staff from access or use of information from the video surveillance system, it's components, files, or database for personal reasons.

With the exception of records retained for criminal, safety, or security investigations or evidentiary purposes, or as otherwise required by law, the Municipality must not maintain a copy of recordings for longer than 30 days.

Any records that are accessed or disclosed will be retained for one year, as per Regulation 460 of FIPPA and section 5 of Regulation 823 of MFIPPA.

The Municipality will take all reasonable efforts to ensure the security of records in its control / custody and ensure their safe and secure disposal.

Old storage devices must be disposed of in accordance with an applicable technology asset disposal process ensuring personal information is erased prior to disposal, and cannot be retrieved or reconstructed. Disposal methods may include shredding, burning, or erasing, depending on the type of storage device.

Unauthorized Access and/or Disclosure (Privacy Breach)

Staff who become aware of any unauthorized disclosure of a video record in contravention of this Policy and/or a potential privacy breach are to immediately notify the Director of Physical Services and the Chief Administrative Officer. After this unauthorized disclosure or potential privacy breach is reported:

- Upon confirmation of the existence of a privacy breach, the Chief Administrative Officer shall notify the Information and Privacy Officer of Ontario (IPC) and work constructively with the IPC staff to mitigate the extent of the privacy breach and to review the adequacy of privacy protection with the existing policy.
- The Director of Physical Services shall inform the Chief Administrative Officer of events that have led up to the privacy breach.
- The staff member shall work with the Director of Physical Services to take all reasonable actions to recover the record and limit the record's disclosure.
- The Director of Physical Services will notify affected parties whose personal information was inappropriately disclosed.
- The Director of Physical Services shall investigate the cause of the disclosure with the goal of eliminating potential future occurrences.

Intentional wrongful disclosure or disclosure caused by negligence by employees may result in disciplinary action up to and including dismissal. Intentional wrongful disclosure or disclosure caused by negligence by service providers (contractors) may result in termination of their contract.

Inquires From the Public Related to the Video Surveillance Policy

A staff member receiving an inquiry from the public regarding the Video Surveillance Policy shall direct the inquiry to the Chief Administrative Officer.

Review of Video Surveillance Policy

This policy shall be reviewed every 2 (two) years by the Chief Administrative Officer who will forward recommendations for update, if any, to Council for approval.

Appendix 1 - Law Enforcement Officer Request Form

RELEASE OF RECORD TO LAW ENFORCEMENT AGENCY UNDER SECTION 32(G) OF THE MUNICIPAL FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT.

I, _____, of the _____
(print name of officer) (print name of police force)

request a copy of the following record(s):

1.

2.

3.

containing the personal information of _____
(print name(s) of individual(s))

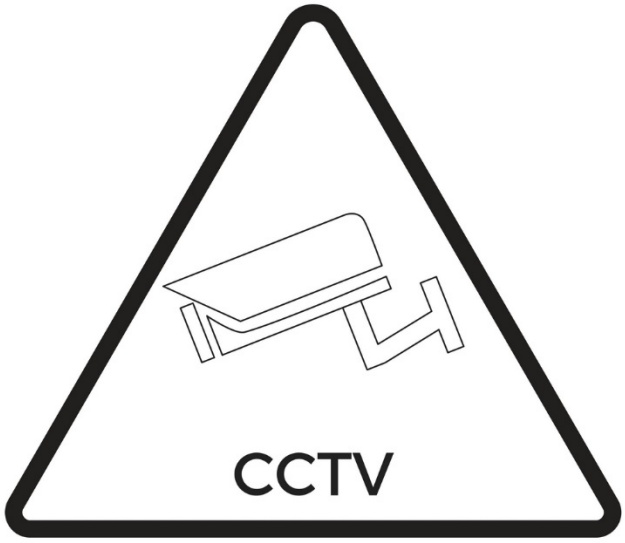
to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

_____	_____	_____
Signature of Officer	Badge/Identification No.	Date

_____	_____
Signature of Director of Physical Services	Date

Return all completed ORIGINAL forms to the Director of Physical Services at the Municipality of Central Elgin, 450 Sunset Drive, Elgin County Administration Building, St. Thomas, Ontario N5R 5V1.

Appendix 2 – Notice of Collection



ATTENTION

This area may be monitored by Video Surveillance Cameras

The personal information obtained from the Video Surveillance Cameras at this site is collected under the legal authority of the The Municipal Act, 2001, and . The information you provide may be used for the purpose of promoting public safety and reduction of crime at this site.

Any questions about this collection can be directed to the CAO at 450 Sunset Drive, St. Thomas, or 519-631-4860. More information is available at www.centralelgin.org.