

## POLICY

<b>Name of Policy:</b> <b>VIDEO SURVEILLANCE POLICY</b>	<b>Policy Number:</b> <b>008</b>
<b>Resolution Number:</b> <b>2021/08/240</b>	<b>Approval Date:</b> <b>AUGUST 17, 2021</b>
<b>Administrative Responsibility:</b> <b>FIRE CHIEF</b>	<b>Next Review Date:</b> <b>AUGUST 2025</b>

## Policy Statement

The Corporation of the Municipality of Callander (the “Municipality”) is committed to public safety, crime prevention, and stewardship of publicly owned assets. Where warranted, the Municipality may use video surveillance systems, on municipal property, for the express purposes of enhancing safety and security of all persons and municipal property, including preventing and deterring crime such as, but not limited to, theft, vandalism, and unauthorized entry. The video surveillance can also aid in identifying suspects and gathering evidence. The Municipality shall always maintain control of and responsibility for its video surveillance system.

This policy does not imply or guarantee that a camera or recording equipment will be monitored in real time 24 hours a day, seven days a week. The Municipality will only permit the use of video surveillance equipment for the purpose of safety and security of persons and property. To be clear, video surveillance equipment will only be used, by the Municipality, for law enforcement and crime prevention purposes.

## Purpose

The purpose of this Policy is to outline the responsible use of video surveillance equipment, used by the Municipality, for recording, monitoring, and storing video images.

The Municipality of Callander recognizes the need for synergies between an individual's right to privacy and the Municipalities duty to promote and maintain a safe and secure environment. The use of video surveillance equipment results in the collection of personal information in the form of images (both still and live) of individuals and conduct. This policy is to guide how the Municipality will control surveillance and the collection of, maintenance of, and access to and surveillance records.

## Definitions

“Municipality” means the Corporation of the Municipality of Callander.

“Law Enforcement” means,  
(a) policing,

- (b) investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, or
- (c) the conduct of proceedings referred to in clause (b).

*“Personal Information”* means recorded information about an identifiable individual, including,

- (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- (c) any identifying number, symbol or other particular assigned to the individual,
- (d) the address, telephone number, fingerprints, or blood type of the individual,
- (e) the personal opinions or views of the individual except if they relate to another individual,
- (f) correspondence sent to the *Municipality* by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
- (g) the views or opinions of another individual about the individual, and
- (h) the individual’s name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

*“Record”* means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes,

- (a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine-readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof, and
- (b) subject to the regulations, any record that is capable of being produced from a machine-readable record under the control of the *Municipality* by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the *Municipality*.

*“Video Surveillance Equipment”* means cameras and recording equipment used to record and store video images. Cameras are deployed in an overt and fixed (non-mobile) manner without the use of video analytics. The equipment does not record and store sound.

#### Legislative & Administrative Authorities

- Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56 (MFIPPA)
- Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31
- Guidelines for the Use of Video Surveillance - Information and Privacy Commissioner of Ontario (October 2015)

#### Policy Requirements

### DESIGN, INSTALLATION, AND OPERATION OF THE VIDEO SURVEILLANCE SYSTEM

In designing, installing, and operating the video surveillance system, the following must be considered:

- Cameras are only installed in identified public areas where municipal staff determines it necessary for the protection of municipal property, deterrence, and detection of unlawful activities.
- The installation is justified based on specific reports of incidents of crime, vandalism, inappropriate behaviour, and safety concerns.
- The equipment will operate 24 hours/seven days a week, within the limitations of system capabilities.
- Camera adjustments shall be made so that images of private property are not recorded. Only images on municipal property shall be recorded.
- Video surveillance equipment is not to be used to routinely monitor municipal employees.
- Video reception equipment (e.g., monitors) shall be kept in a controlled area and away from the public. Only authorized persons have access to the video reception equipment.
- Clearly written signs shall be prominently displayed providing the public with adequate warning that video surveillance is in effect.
- Signs shall meet the requirements of the Municipal Freedom of Information and Privacy Act s.29(2).

## **ACCESS**

Only authorized staff shall be permitted to access the video surveillance equipment and stored records.

The Municipality shall not use personal information in its custody or under its control except,

- (a) if the person to whom the information relates has identified that information in particular and consented to its use;
- (b) for the purpose for which it was obtained or compiled or for a consistent purpose; or
- (c) for a purpose for which the information may be disclosed to the institution under section 32 or under section 42 of the *Freedom of Information and Protection of Privacy Act*. R.S.O. 1990, c. M.56, s. 31.

A log (Video Surveillance System Review Log) listing all instances where the video surveillance records are reviewed shall be kept enabling a proper audit trail. The log shall identify who conducted the review, those present, date, time, and purpose of review.

Each time authorized staff review video surveillance records they shall make an entry in the Video Surveillance System Review Log.

## **DISCLOSURE**

The Municipality shall not disclose personal information in its custody or under its control except,

- (a) in accordance with Part I of MFIPPA;
- (b) if the person to whom the information relates has identified that information in particular and consented to its disclosure;
- (c) for the purpose for which it was obtained or compiled or for a consistent purpose;

- (d) if the disclosure is made to an officer, employee, consultant, or agent of the Municipality who needs the record in the performance of their duties and if the disclosure is necessary and proper in the discharge of the Municipalities functions;
- (e) where permitted or required by law or by a treaty, agreement or arrangement made under an Act or an Act of Canada;
- (f) if disclosure is by a law enforcement institution,
  - (i) to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty or legislative authority, or
  - (ii) to another law enforcement agency in Canada;
- (g) to a Municipality or a law enforcement agency in Canada if,
  - (i) the disclosure is to aid in an investigation undertaken by the Municipality or the agency with a view to a law enforcement proceeding, or
  - (ii) there is a reasonable basis to believe that an offence may have been committed and the disclosure is to enable the Municipality or the agency to determine whether to conduct such an investigation;
- (h) in compelling circumstances affecting the health or safety of an individual if upon disclosure notification is mailed to the last known address of the individual to whom the information relates;
- (i) in compassionate circumstances, to facilitate contact with the spouse, a close relative or a friend of an individual who is injured, ill or deceased;
- (j) to the Minister;
- (k) to the Information and Privacy Commissioner;
- (l) to the Government of Canada or the Government of Ontario in order to facilitate the auditing of shared cost programs. R.S.O. 1990, c. M.56, s. 32; 2006, c. 19, Sched. N, s. 3 (5); 2006, c. 34, Sched. C, s. 15; 2019, c. 7, Sched. 41, s. 2.

Video surveillance records disclosed to another agency shall be limited only to the specific incident under investigation. Two copies of the incident shall be made – one shall be provided to the investigating agency and the other copy shall be retained by the Municipality.

Video Surveillance records are kept on a hard drive. Should the investigating agency require the entire contents of the hard drive they shall be required to provide the Municipality with a warrant before the entire contents are released.

Prior to releasing a copy of the incident to the investigating agency, the Storage Device Release Form must be completed.

## **RETENTION**

To ensure that individuals have a reasonable opportunity to access the personal information about them held by institutions, FIPPA, MFIPPA and their regulations set out rules regarding the minimum length of time Municipalities must retain personal information once they have used it. Specifically, section 5(1) of Regulation 460 of FIPPA and section 5 of Regulation 823 of MFIPPA require Municipalities, in general, to retain personal information for at least one year after use.

It is important to note that this retention requirement applies only to personal information that has been “used” by the Municipality. It does not apply to personal information that has been collected but not used, which in the case of video surveillance may have much shorter retention requirements.

The video surveillance recording equipment will retain data for thirty (30) days. Then automatically overwrite over the old data.

In the context of video surveillance, personal information is used whenever footage that contains images of individuals or other identifiable information is accessed. However, simply viewing a live feed does not represent a “use” of personal information.

Video surveillance footage that has been used for an investigation or disclosed, to another agency, shall be retained for one (1) year from the date of viewing.

## **SECURITY AND DISPOSAL OF VIDEO SURVEILLANCE RECORDS**

Any person(s) who tampers with or destroys video surveillance equipment may be subject to sanctions which could include criminal proceedings.

Storage devices that are no longer functioning must be destroyed/erased in a manner that the personal information cannot be reconstructed or retrieved. That may include shredding, burning or magnetically erasing the personal information.

## **BREACH OF INFORMATION**

If a privacy breach has occurred (loss, theft, or inadvertent disclosure of personal information) the Municipality shall ensure that inadvertent disclosures are addressed in a timely and effective way.

The Senior Municipal Director and the Municipal Clerk must be notified as soon as a breach has been discovered.

The Municipal Clerk shall respond to any inadvertent disclosures of personal information.

The Municipal Clerk shall contact the Freedom and Information and Privacy Office and advise of any significant breach of personal information.

The Municipal Clerk shall identify the scope of the breach and take steps to contain the damage.

If applicable, individuals whose personal information has been disclosed shall be notified.

The Municipal Clerk shall conduct an internal investigation and implement, based on the findings, any required changes.

## **ANNUAL AUDIT & EVALUATION**

The Fire Chief shall conduct an annual review of the video surveillance policy to ensure that:

1. Review the policy to ensure full compliance.
2. Video surveillance continues to be justified and, if so, whether its use can be restricted.
3. Logbooks, disclosure release forms, and disposal records are properly maintained.
4. Requirements for retention of records are being followed.

5. Any formal or informal information requests from the public have been tracked.

#### Staff Responsibilities

**The Fire Chief** shall be responsible for implementation, administration, and evaluation of the Municipalities Video Surveillance Policy. He/she shall also determine staff that are authorized to access the video surveillance equipment. The Fire Chief shall be responsible for ensuring that information obtained through video surveillance is used exclusively for lawful purposes.

**Staff with authorized access** to the video surveillance equipment and recorded information shall be trained in its use in accordance with this policy. Training shall include review of the policy, review of the relevant legislation and proper use of the video surveillance equipment. Authorized staff shall sign a written confidentiality agreement regarding their duties under the Policy and the Acts. Breaches of the policy may result in disciplinary action in accordance with the Municipalities Progressive Discipline Policy.

**The By-law Enforcement Officer(s)** shall act as a liaison with agencies requesting access to the video surveillance data.

**The Municipal Clerk** is responsible for all Municipal Freedom of Information requests.



## APPENDIX A

## VIDEO SURVEILLANCE SYSTEM REVIEW LOG

[illegible]



## APPENDIX B

### SURVEILLANCE VIDEO RELEASE FORM

This form is used to release Municipality of Callander video surveillance data. This must be completed each time video surveillance data is released.

DATE (MM/DD/YYYY)	TIME (HH:MM)	CAMERA		DATE/TIME RANGE OF DATA

Type of Media Used (USB, CD/DVD): \_\_\_\_\_

(Note: Email or any form of online sharing is not to be used)

NAME OF AUTHORIZED PERSON RELEASING DATA (PRINT):	POSITION:	SIGNATURE

Purpose or Reason for Release:

---

---

---

---

Name of Person Taking Custody of Copy of Video Surveillance Data (print):

\_\_\_\_\_

#### Acknowledgement of Receipt and Indemnity

I, the above noted individual, on behalf of my employer, acknowledge receipt of a Municipality of Callander surveillance video and agree that I and my employer will hold the Municipality of Callander harmless for any damage that occurs due to the release of the surveillance video while in my custody or under my control.

\_\_\_\_\_

Signature

Position	Badge or ID#	Agency	Phone Number

#### Disposition Following Use:

☒ To be destroyed    ☐ To be returned to Municipality    ☐ Other (specify): \_\_\_\_\_



[illegible]