Town of Whitby Procedure

Procedure Title:	Surveillance Systems Procedure
Procedure Number:	CA 030-005
Reference:	Information Governance Policy (CA 030) Corporate Access and Privacy Policy (CA 060) Privacy Breach Protocol (CA 060-002) Records Classification and Retention Bylaw No.7707-20
Date Approved:	September 13, 2024
Date Revised:	n/a
Approval:	Chief Administrative Officer
Point of Contact:	Supervisor, Corporate Security Manager, Records & Privacy

Purpose

The purpose of this procedure is to oversee and manage the use of Surveillance Systems by the Town of Whitby to ensure their appropriate compliance with Town policies, procedures and applicable legislation.

Scope

This procedure applies to:

- All Town staff and contractors, including any individual or entity permitted to use or have access to a Surveillance System; and
- Any Surveillance System installed by the Town whether on or outside of Town owned, operated or leased facilities, properties or assets.

This procedure does not apply to:

- Recordings and livestream of Town Council, Committee or other meetings facilitated by the Town that are open to the public; and,
- Surveillance Systems where no Personal Information is collected, stored, used or disclosed by the Town.

Index

1. Definitions

1.1. **Authorized Personnel** means a designated individual who is permitted to gain access to Surveillance Systems and to undertake one or more of the following functions: to retrieve, download, view, secure, copy, distribute and/or destroy Recordings.

1.2. **Covert** means concealed or hidden.

1.3. **MFIPPA** means the *Municipal Freedom of Information and Protection of Privacy Act*.

1.4. **Personal Information** means information about an identifiable individual, as defined in section 2(1) of the MFIPPA.

1.5. **Recordings** means the data (image and video) that is livestreamed, created and/or stored as a result of the use of a Surveillance System.

1.6. **Surveillance System** means equipment capable of recording or monitoring through images or video for purposes related to the safety or security of individuals or to protect or manage Town property.

2. Responsibilities

2.1. **Commissioner of Community Services:**

2.1.1. Approve the use of Covert Surveillance Systems for limited and case-specific circumstances.

2.2. **Supervisor, Corporate Security:**

2.2.1. Responsible for the overall review, approval, implementation, maintenance and audits of Surveillance Systems.

2.2.2. Provide appropriate training to Authorized Personnel on the responsible use of applicable Surveillance Systems.

2.2.3. In consultation with Technology and Innovation Services and Manager, Records & Privacy, manage the secure storage and destruction of Recordings in accordance with the Records Classification and Retention Bylaw.

2.2.4. Responsible for conducting security reviews of Town Sites where Surveillance Systems are being considered for installation.

2.2.5. Respond to requests from law enforcement agencies for access to Recordings under MFIPPA.

2.3. Office of the Town Clerk:

2.3.1. Assist with conducting risk review and privacy impact assessments on Surveillance Systems.

2.3.2. Respond to requests from the public or law enforcement agencies for access to Recordings under MFIPPA.

2.4. Authorized Personnel:

2.4.1. Review and understand this procedure prior to using any Surveillance or Monitoring System or accessing Recordings.

2.5. All Town Staff and Contractors:

2.5.1. Responsible for complying with this procedure and reporting any violations of this procedure to a Supervisor or Manager.

2.5.2. Will not access, use or disclose Recordings for personal reasons, nor dispose, destroy, erase or alter any Recording without proper authorization and without following this procedure.

3. Security Risk Review and Privacy Impact Assessment

3.1. If a new Surveillance System is being considered, or if significant changes occur to an existing one, a security risk review shall be completed and a privacy impact assessment may be completed prior to installation. While conducting a privacy impact assessment is considered a best practice, Staff shall consider the scope of the project, timing, staffing resources, surveillance objectives, and any other relevant considerations when deciding whether or not to conduct a privacy impact assessment.

3.2. The security risk review shall, at a minimum, consider:

3.2.1. Whether the proposed Surveillance System is justified on the basis of verifiable or specific reports of incidents of crime or safety or security concerns for individuals or Town property or assets.

3.2.2. Other measures and determine those other measures are not feasible or are substantially less effective than a Surveillance System, and that the benefits of the Surveillance System outweigh the reduction of privacy.

3.3. If conducted, the privacy impact assessment shall be based on the requirements of MFIPPA and may review and make recommendations on:

3.3.1. The collection, use, disclosure and retention of Personal Information;

3.3.2. The requirements for notice and individual access; and

3.3.3. Appropriate measures to safeguard Personal Information.

4. Installation of Surveillance Systems

4.1. The installation or use of Surveillance Systems shall be based on the security risk review and privacy impact assessments and be limited to the locations that have been identified as requiring surveillance or monitoring.

4.2. The installation or use of Surveillance Systems shall:

4.2.1. Not be pointed directly at windows in adjacent buildings or homes, or record areas where individuals have a higher expectation of privacy, such as change rooms and washrooms.

4.2.2. Minimize privacy intrusions to that which is absolutely necessary to achieve its required and lawful goals.

4.2.3. Where applicable, restrict camera adjustments (e.g. tilt, pan, zoom) to ensure operators cannot adjust or manipulate cameras to monitor or record unauthorized areas.

4.3. Notice of the use of Surveillance Systems shall be provided prior to being used and shall:

4.3.1. Satisfy the notification requirements under Section 29(2) of MFIPPA.

4.3.2. Be provided in the format(s) most effective to notify the individuals who may have their Personal Information recorded or monitored (e.g. signs, information posted on Whitby.ca).

4.3.3. If using signs, use clear, language-neutral graphical depiction of the use of the Surveillance System and have the signs prominently displayed at the entrances, exterior walls, interior of buildings and/or perimeter of the surveillance or monitored areas.

4.3.4. The following wording is recommended for Surveillance System signage at the Town of Whitby but may be revised on a site-by-site bases to reflect specific uses of surveillance system:

CCTV Camera in Use:
Under the authority of the Municipal Act, 2001.
Video footage will be used to promote
public safety and reduce crime.

Questions: Town of Whitby Clerk
905-430-4300
clerk@whitby.ca

4.4. Section 4.3 of this procedure does not apply to approved Covert Surveillance Systems used for law enforcement purposes or where Regulations 823 made under MFIPPA provides that the notice is not required.

5. Management of Recordings

5.1. Authorized Personnel

5.1.1. Authorized Personnel shall be limited to specific individuals who legitimately require access to a Surveillance or Monitoring System to retrieve, download, view, secure, copy, distribute and/or destroy Recordings, as may be required in the performance of their duties at the Town or on behalf of the Town.

5.1.2. The following Town staff, or their designate(s), shall be considered Authorized Personnel:

5.1.2.1 Supervisor, Corporate Security

5.1.2.2 In the absence of the Supervisor, Corporate Security, the Sr. Manager, Facility Operations and/or the Director of Facilities

5.2. Access, Use and Disclosure of Recordings

5.2.1. Recordings shall only be accessed, used or disclosed for the purpose(s) for which it was collected or for a consistent purpose, or for any other access, use or disclosure permitted by MFIPPA.

5.2.2. Any access, use or disclosure of Recordings that are in contravention of this procedure and/or a potential privacy breach shall be immediately reported to the Manager, Records & Privacy.

5.3. Retention, Storage and Destruction of Recordings

5.3.1. Records that are used shall be considered and managed as official records and shall be retained in accordance with the Records Classification and Retention Bylaw. For reference purposes only, the following are applicable classification and retention periods:

5.3.1.1 Town Facility - Property Security Administration (AM44) is kept for five (5) years from the date of export

5.3.1.2 Records related to Law Enforcement would be filed under the appropriate incident categorized under Enforcement - Enforcement Actions (LC10) and kept for 10 years from the date of the incident

5.3.1.3 Access & Privacy - Freedom of Information Requests (GV01) would be kept for 5 years from the date of close of the request

5.3.1.4 Legal Hold – Keep until resolved

5.3.2. Recordings that are not used shall be destroyed at such time when the Surveillance System is programmed to automatically overwrite the Recording.

5.3.3. The retention period for unused Recordings is up to 120 days and shall be limited to the amount of time reasonably necessary to discover or report an incident that occurred in the space or audio under surveillance.

5.3.4. All Recordings shall be stored and labelled with appropriate metadata (e.g. dates, times, locations, caller identification, unique or sequential numbers, etc.) to allow for the accurate and timely retrieval of Recordings and to support their lifecycle management.

5.3.5. When destroying or overwriting Recordings, it shall be done in such a way that the Personal Information contained in the Recordings cannot be reconstructed or retrieved in any way.

5.4. Security of Recordings

5.4.1. All Surveillance System equipment and recordings shall be kept in a secure and controlled access area that is only accessible to Town Staff.

5.4.2. Every reasonable attempt should be made to ensure unauthorized individuals do not view Recordings from Surveillance Systems.

6. Auditing and Evaluation Surveillance Systems

6.1. Surveillance Systems shall, at minimum, be audited annually to evaluate their compliance with this procedure and to determine whether their existence continues to be justified in accordance with subsection 3.2.1. of this procedure.

6.2. Any deficiencies or concerns identified by the audit shall be addressed immediately or as soon as reasonably practical.

7. Transition of Legacy Surveillance Systems

7.1. Surveillance Systems not in compliance with this procedure shall be brought into compliance within a reasonable period of time following the approval of this procedure, as determined by the Commissioner of Community Services.

Original Approved and Signed.

Matthew Gaskell, Chief Administrative Officer, x2211

September 13, 2024

Date