CORPORATION OF THE TOWNSHIP OF ESQUIMALT

COUNCIL POLICY

TITLE: VIDEO SURVEILLANCE	NO. ADMIN - 76

POLICY:

1. Policy Overview

The Township of Esquimalt (the Township) recognizes the need to balance an individual's right to privacy and the need to ensure the public safety and security of Township staff, clients, visitors, facilities and properties.

As a public body governed by the *Freedom of Information and Protection of Privacy Act* (FIPPA), the Township has obligations with respect to notice, access, use, disclosure, retention and disposal of records. While video surveillance cameras are installed for public safety and security reasons, the Township's video surveillance system 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 the Township's facilities and properties operating in a way that protects public safety, security, and privacy. Personal information collected by the Township's video surveillance system includes video images only and does not include any audio recordings.

2. Policy Description

This Policy has been developed to govern video surveillance at Township owned and leased properties in accordance with the privacy provisions of FIPPA.

This Policy has been drafted to conform to practices outlined by the Office of the Information and Privacy Commissioner for British Columbia (OIPC) in a document entitled "Public Sector Surveillance Guidelines", available at https://www.oipc.bc.ca/guidance-documents/1601.

3. Definitions

"Video Surveillance System" includes all of the various components of the Township's video surveillance process used to record digital images, to connect to the Township's internal secure website, and to view, store, retain, provide access to and dispose of such digital images.

"Equipment" includes the video recording cameras that digitally record images, the digital video recorder (DVR) on which recorded images are temporarily stored, the surveillance monitors on which the recorded images can be viewed, and the internal server on which the recorded images are retained during the specified period.

"Record" means the recorded digital material and electronic images produced by the Equipment.

4. Application

This Policy applies to the Video Surveillance System implemented by the Township at Township owned and leased properties for public safety and security purposes. The Policy is applicable to all staff of the Township, its elected officials, service providers and contractors that may have access to the Video Surveillance System, the Equipment or the Record.

This Policy does not apply to:

i) video surveillance by the Victoria Police;

ii) video surveillance for employment or labour relations purposes; or

iii) video surveillance of roads in order to assess their condition, for reduction of liability purposes.

5. Responsibilities

1. Information Technology Manager

The Information Technology Manager (IT Manager) or his or her designate is the senior staff member responsible for the administration of this Policy.

The key duties of the IT Manager include:

- Ensuring Policy compliance and providing status updates to the CAO annually regarding compliance with the Policy.
- Undertaking regular evaluations of the Township's Video Surveillance System to ensure compliance with this Policy.
- Subject to prior approval by the CAO, approving the installation of video recording cameras at specified locations on Township owned and leased properties.
- Ensuring proper public notification is provided including appropriate placement of signage.
- Overseeing day-to-day operations of the Video Surveillance System.
- Ensuring all Records and Equipment are stored in a safe and secure location and that access is restricted to authorized staff only.
- Immediately reporting to the Corporate Officer any unauthorized access to or disclosure or copying of Records or any alleged privacy breach, and working with the Corporate Officer to investigate all such occurrences.

2. Corporate Officer

   As the Head for the purposes of FIPPA, the Corporate Officer is responsible for providing a response to access requests and for investigating and reporting any alleged privacy breaches to OIPC.

   The key duties of the Corporate Officer include:

   - Acting as the primary contact for all requests by law enforcement agencies or by members of the public for access to Records.
   - In consultation with the Director of Corporate Services and Human Resources, providing training on obligations and compliance with FIPPA and this Policy to any staff that is to be authorized to be involved with any part the Video Surveillance System, such training to occur prior to such staff being provided access to any part of the Video Surveillance System.

3. Director of Parks and Recreation Services

   The Director of Parks and Recreation Services is responsible for promoting public safety and security and reducing property damage at Township recreation facilities.

   The key duties of the Director of Parks and Recreation Services include:

   - Ensuring the appropriate placement of video surveillance equipment that is justified on the basis of verifiable, specific reports of incidents of significant public safety or security concerns.
   - Removing video surveillance equipment from locations no longer meeting the justifications for initially installing it.
   - Conducting investigations or working with local police services where property damage to Township facilities or assets or other unlawful activity has occurred.

4. Other Staff

   In addition to the IT Manager, Corporate Officer, and Director of Parks and Recreation Services, only staff designated by the CAO shall be permitted to operate the Video Surveillance System or to have access to the Equipment or Records, and only after they have been appropriately trained.

   The key duties of other authorized staff include:

   - Staff provided access any part of the Video Surveillance System, Equipment or Records must comply with this Policy.
   - Staff must not access or use any information contained in any Record for personal or other purpose except as authorized under this Policy.
   - Staff must not copy, dispose, destroy, erase or alter any Record.

6. 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 a Video Surveillance System at a specific location should be justified on the basis of verifiable, specific reports of incidents of significant public safety or security concerns.
- A Video Surveillance System should only be considered after other measures of deterrence or detection have been considered and rejected as being unfeasible or significantly less effective.
- An assessment must be conducted on the effects that the proposed Video Surveillance System at a specific location 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 System should minimize privacy intrusion.

In order to minimize privacy intrusion, when designing a Video Surveillance System and installing Equipment, the following must be considered:

- The Equipment should be installed to only monitor those areas that have been identified as requiring video surveillance.
- The ability to adjust or manipulate video recording cameras is restricted so that the cameras do not record areas that are not intended to be covered by the Video Surveillance System, such as through windows in adjacent buildings or onto adjacent properties.
- Equipment should never monitor or record the inside of areas where the public and staff have a higher expectation of privacy (e.g. change rooms and washrooms).
- Video surveillance should be restricted to periods when there is a demonstrably higher likelihood of significant public safety or security concerns in the area under surveillance.
- Viewing and recording equipment must be located in a restricted access area where only authorized staff have access.

7. Public Notification

In order to provide notice to the public and staff that a Video Surveillance System is in use at a particular location:

- The Township shall post signs, substantially as set out in Appendix 1 of this Policy, at all entrances and/or prominently displayed in proximity to the area under video surveillance.
- The notification will also be posted on the Township's website for the public's information.
- The notification must inform individuals of the legal authority for the collection of personal information, the principal purposes for which the personal information is intended to be used, and the Corporate Officer's contact information in the event of any questions about the collection of personal information.

8. Equipment

Any monitors that may be used for viewing of Records will be kept in a secure access-restricted location where they are not visible to the public or unauthorized staff.

All Equipment that is not in use must be stored securely in a locked receptacle located in an access-restricted area.

The IT Manager shall ensure that any Equipment used in the Video Surveillance System is disposed of in accordance with an applicable technology asset disposal process ensuring personal information is erased prior to disposal so that such personal information cannot be retrieved or reconstructed. Acceptable disposal methods may include shredding, burning, or erasing, depending on the type of Equipment. The IT Manager shall prepare a record of the details of the secure destruction of the Equipment.

9. Records

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

The IT Manager shall ensure that, whenever possible, all Records are strongly encrypted when transmitted across open public networks, and are stored in a safe and secure locked location with access restricted to authorized staff only.

The Township shall at all times retain custody and control of all original Records, and any person provided with access shall be provided a copy of the relevant Record.

All Records shall be clearly identified as to the date and location of origin, using a unique, sequential number or other verifiable symbol, as determined by the IT Manager.

The IT Manager shall ensure that, except for Records disclosed pursuant to a request for access to records under FIPPA or retained for public safety or security or criminal investigations or evidentiary purposes, or as otherwise required by law, the Township does not retain the original or a copy of any Record for longer than 30 days. The IT Manager shall ensure that the Video Surveillance System automatically overwrites a Record within 30 days unless the Record is flagged for a longer retention.

Any Records that are accessed or disclosed under FIPPA shall be securely retained by the Township for the required period in accordance with the Township's Records Management Policy.

10. Access to Records and Equipment

Access to Records and Equipment shall be restricted to authorized staff only in accordance with their roles and responsibilities as outlined in this Policy.

All requests for access to Records are to be directed to the Corporate Officer, Municipal Hall, at 1229 Esquimalt Road, Esquimalt, BC V9A 3P1 for response. Such requests must be in writing either in the form of a letter, an email, or on the prescribed form available on the Township's website, and must set out the specific date and time of the incident and Record requested.

The IT Manager shall ensure that a logbook is prepared and retained in a safe and secure location to record all access activities related to Equipment and Records. The activities to be recorded shall include the authorized staff involved, the date, time and details of the activity, and all information regarding the use, maintenance, storage and all instances of access to Records and Equipment.

In the event that the Corporate Officer provides access to any Record, the following information, as relevant, will be recorded by the IT Manger in the 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 prepared and sealed;

iii) the time and date the sealed copy of the Record was provided to the applicant;

iv) the case file number of the Law Enforcement Officer's investigation, if applicable;

v) a description of the circumstances and legal authority justifying the disclosure;

vi) the amount of the Record involved; and

vii) the means used to provide access to the Record.

11. Unauthorized Access (Privacy Breach)

Staff who become aware of any unauthorized access to or disclosure of a Record in contravention of this Policy and/or a potential privacy breach are to immediately notify the Corporate Officer, who will ensure that the following procedures are immediately completed:

i) Upon confirmation of a privacy breach, in accordance with the requirements of FIPPA, the Corporate Officer shall notify the OIPC of the details of the breach.

ii) Together with the IT Manager, the Corporate Officer shall take reasonable steps to mitigate the extent of the privacy breach and review the adequacy of privacy protection measures included in the Video Surveillance System and the existing Policy.

iii) The Corporate Officer shall inform the CAO of any alleged privacy breach.

iv) The IT Manager shall take all reasonable actions to recover the Record and limit any further unauthorized disclosure.

v) The IT Manager shall thoroughly investigate the cause of the unauthorized access or disclosure and take reasonable steps to eliminate potential future re-occurrences.

vi) The Corporate Officer will notify affected parties whose personal information was inappropriately disclosed.

Intentional wrongful disclosure or disclosure resulting from negligence by staff may result in disciplinary action up to and including dismissal. Intentional wrongful disclosure or disclosure resulting from negligence by service providers or contractors may result in termination of their contract.

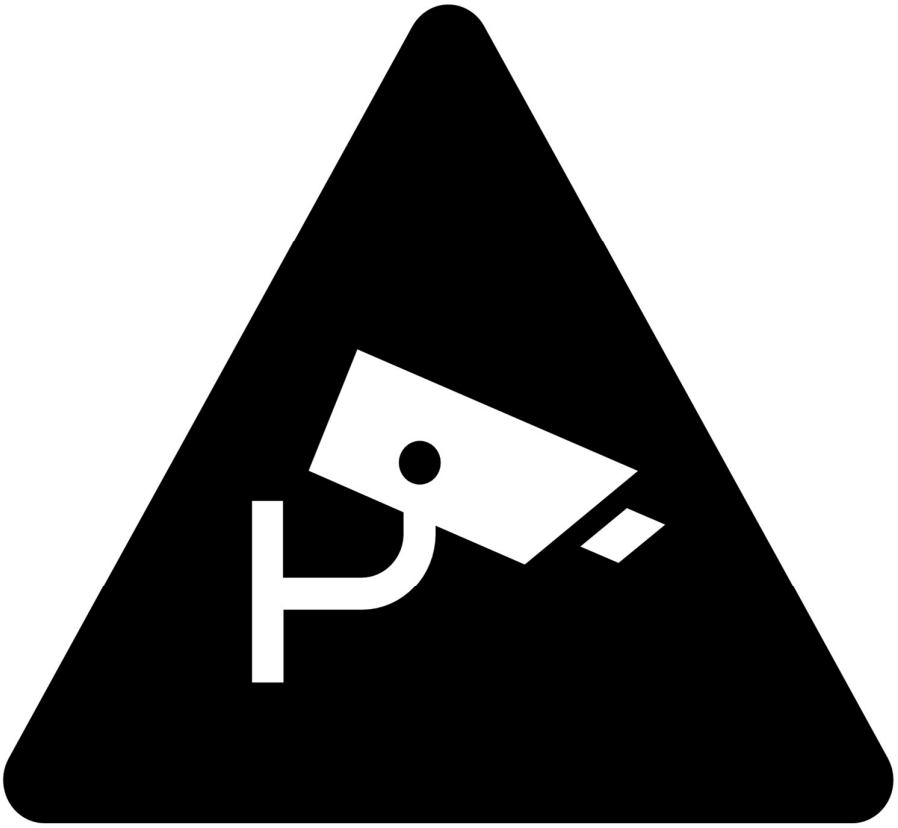
12. Inquiries Related to Policy

All inquiries regarding this Policy shall be directed to the Corporate Officer.

13. Review of Policy

This Policy shall be reviewed annually by the CAO who will forward recommendations for update, if any, to Council for approval.

Appendix 1 – Notice of Video



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 authority of the *Community Charter* and will only be used for the purposes of promoting public safety and security and reducing property damage at this site.

Any questions about the collection of personal information may be directed to the Corporate Officer, Township of Esquimalt, 1229 Esquimalt Road, Esquimalt, BC V9A 3P1, or by telephone at 250-414-7135. More information is available at www.esquimalt.ca.