CORPORATE POLICY

| | |
|---|---|
| **Section:** | Administration |
| **Policy Title:** | **Video Surveillance Policy** |
| **Policy No.:** | A09-CORP-005 |
| **Approved By:** | Council |
| **Effective Date:** | 2024- 12-19 |
| **Revised Date:** | |

# VIDEO SURVEILLANCE POLICY

## 1 POLICY STATEMENT

1.1 The Township of Malahide recognizes the delicate balance between an individual's right to be free from invasion of privacy, and the need to protect the safety and security of its employees, the public, and property. In respecting this balance, the Township is committed to ensuring and enhancing the safety and security of the public and its employees, and stewardship of public property, by integrating security best practices with the responsible use of technology. Employees ensure the personal information of persons captured on video surveillance is maintained as private, confidential and secure, except as legally exempted or in situations outlined in this policy.

## 2 PURPOSE

2.1 To establish guidelines which will promote and foster a safe and secure environment for residents and staff, to ensure public safety for community members who visit or use Township facilities or parks, and to mitigate the risk of personal and municipal loss or destruction of property.

## 3 DEFINITIONS

3.1 Authorized Personnel means Employees authorized by the CAO to view, access and make a Record of Video Surveillance footage.

3.2 Facility means any building or land that is either owned or leased by the Township.

3.3 Individual Requests means request(s) for a Record made by a member of the public under the provisions of MFIPPA but excludes a request made by law enforcement.

3.4 IPC means Information and Privacy Commissioner of Ontario.

3.5 Law Enforcement Requests means request(s) for a Record made by a law enforcement agency.

3.6 MFIPPA means Municipal Freedom of Information and Protection of Privacy Act. Private Property means building structures or property not owned, leased, or rented by the Township.

3.7 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 the 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 an institution 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.

3.8 Record means any unit of information however recorded, whether in printed form, on film, by electronic means, or otherwise, and includes correspondence, memoranda, plans, maps, drawings, graphic works, photographs, film, microfilm, sound recordings, videotapes, machine readable records, an e-mail and any other documentary material regardless of physical form or characteristics, made or received in the course of the conduct of Township business.

3.9 Retention period is the period of time during which a specific records series must be kept before records in that records series may be disposed of.

3.10 Township means the Corporation of the Township of Malahide

## 4 RESPONSIBILITIES:

4.1 CAO shall:

- Determine authorized personnel to view, access and make a Record of Video Surveillance footage under this policy;

- Authorize installation of security cameras and surveillance practices; and
- Provide oversight and compliance with this policy by all Township employees.

4.2 Clerks Department shall:

- Process applications for access to information submitted by individuals under the provisions of MFIPPA and/or law enforcement;
- in conjunction with the HR Department, develop and provide training regarding awareness and compliance with MFIPPA, including employee responsibilities and how to handle information inquiries.
- Conduct periodic audits to ensure full compliance with this policy, IPC guidelines and MFIPPA;
- Respond to requests for disclosure under the Freedom of Information or applicable or routine disclosure procedures;
- Ensure a public notice for video surveillance is placed at all Township sites that have a video surveillance system;
- Respond to requests from the public and employees about the collection, use, and disclosure of personal information captured by a video surveillance system;
- Respond to appeals and privacy complaints received through the Office of the Information and Privacy Commissioner of Ontario (IPC);
- Notify the IPC in the event of a privacy breach, where appropriate; and
- Work with department manager(s) and employee(s) in the event of an improper disclosure of personal information.

4.3 General Manager of IT shall:

- Maintain custody of all Records created by the video surveillance systems;
- Ensures the continued operation and maintenance of security cameras and recording software; and
- Assist Clerks Department as required in the processing of applications for access to information submitted by individuals under MFIPPA;

4.5 Managers and Supervisors shall:

- Ensure the appropriate use of the video surveillance system at their facility(ies) in compliance with this policy;
- Delegate and assign responsibility regarding who will act on their behalf in following procedures relating to this policy in their absence;
- Provide job specific training;
- Refer any requests for copies of surveillance video to the Clerk or Delegated Employees;
- Investigate and report any privacy breaches to the Clerk or Delegated Employees; and
- Ensure that employees are monitoring compliance with the retention periods applicable to the video surveillance systems.

4.4 Employees shall:

- Report to their manager or supervisor any suspected privacy breach;
- Report to their supervisor any problems with the video surveillance system; and
- Review and comply with this policy and MFIPPA in performing their duties and functions related to the operation of the video surveillance system. Employees may be subject to criminal charges, civil liability and/or discipline, including but not limited to termination, for a breach of this policy, or provisions of MFIPPA or other relevant statutes.

## 5 SIGNAGE AND NOTIFICATION:

**5.1** A notice of collection will be posted on the Township website and shall state the following:

a) The legal authority for the collection;

b) The principal purpose or purposes for which the personal information is intended to be used; and

c) The title, business address and business telephone number of a public official who can answer the individual's questions about the collection. Signage will be prominently displayed at the perimeter of the monitored areas and at key locations within these areas. Signage shall include basic information to notify the public and staff of the Township use of video surveillance in the area.

## 6 CAMERA PLACEMENT:

6.1 Camera positions will be determined on the basis of reasonable and justifiable grounds for the provision of safety and security. Each camera position will be assessed on a case-by-case basis to determine the effects the system may have on personal privacy. No camera shall be placed so that it views an area where individuals have a greater expectation of privacy.

## 7 OPERATION OF VIDEO SURVEILLANCE SYSTEMS:

7.1 Video surveillance systems shall be:

- operated by Authorized Personnel only.
- No sound is to be monitored or recorded in connection with the video surveillance system unless it is directly related to the problem to be addressed by the video surveillance.
- Authorized Personnel may monitor real-time camera feeds in accordance with this policy.
    - Video surveillance footage will not be used to monitor patrons' general use of Facilities. Circumstances which warrant review will be limited to security incidents that have been reported to the Township, or in the investigation of an incident or potential crime.

- Video surveillance logs will be kept for all instances of access to, and use of, recorded material to enable a proper audit trail.
- The Township will take all reasonable efforts to ensure the security of Records in its custody and ensure their safe and secure disposal. Disposal methods may include overwriting electronic records, shredding, burning or magnetically erasing the Record, in accordance with the Township retention policies.
- Access to video surveillance systems will be restricted through a confidential password that will be distributed to Authorized Personnel by the General Manager of IT.

## 8 CUSTODY

8.1 The General Manager of IT maintains custody of all Records created by the video surveillance systems. Records will be retained for a time of not more than 365 days from the date of use, after which, the Records shall be destroyed. All Records and logs shall be stored in a secure place to avoid tampering and ensure confidentiality. Surveillance systems will be set-up to ensure DVR recordings are cleared or overwritten on a regular basis. Normally, DVR systems will be set-up to maintain recordings for up to 365 days. When viewing or making a Record of a DVR recording, Authorized Personnel will include the following in the video surveillance log;

- Date and time the recording was accessed;
- Name of the employee viewing or making the record;

  Reason(s) for access;
- Date and Time of the information to which access was allowed; and
- Provisions for the return of the record or its destruction. All records authorized for release by designated staff must be stored on an encrypted device.

## 9 ACCESS

Authorized personnel may only view or make record of video when necessary for a specific purpose, such as for an investigation, security checks, compliance with regulations otherwise or directed to do so by the CAO as a direct result of a request made under MFIPPA.

Individual requests

All requests for access to, and release of video surveillance records shall be subject to MFIPPA and shall be directed to legal and council support services. Clerks Department in cooperation with the General Manager of IT shall process MFIPPA requests, in accordance with the legislation.

Law Enforcement Requests

Records required for the purpose of law enforcement require the requestor to complete a Law Enforcement Access Request Form and forward it to the Municipal Clerk and/or their designate. The Municipal Clerk, or their designate, will then provide the record for the specified date and time of the incident to their requestor subject to compliance with MFIPPA. At minimum the following information will be collected:

- Name of Requestor;
- Investigation Number and Reason for the Request;
- The date and time of the original, recorded incident including the designated name/number of the applicable camera and DVR;
- Name of the authorized personnel making the record;
- Time and date the copy of the original record was encrypted;
- Date and time the encrypted record was provided to the requestor

## 10 APPEAL PROCESS

10.1 There is no additional appeal process at the municipal level. If the Complainant is not satisfied with the results of the investigation or the process, they may contact the Office of the Ontario Ombudsman. The Ontario Ombudsman has the authority to look at how the issue was handled by the Township, the steps taken, and the outcome. The Ombudsman has the authority to consider and make recommendations as to whether the process was fair, transparent, and in accordance with applicable policies and by-laws of the Township.

## 11 UNAUTHORIZED DISCLOSURE:

11.1 If any Township employee has knowledge of an unauthorized disclosure of a record, or any contravention of this policy, the following shall take place:

1. The employee shall immediately inform the CAO and Municipal Clerk

2. The employee shall work with the IT Department and the Municipal Clerk to take all reasonable actions to recover and limit the records disclosure.

3. The Municipal Clerk shall, subject to compliance with MFIPPA, make reasonable efforts to inform the individual(s) whose record(s) was/were disclosed as a result of the breach.

4. The CAO, Clerk, General Manager of IT, and HR Manager shall investigate the cause of the disclosure with the goal of eliminating potential future occurrences.

5. The Township shall take any unauthorized disclosure of information very seriously. It shall be understood that intentional wrongful disclosure, or disclosure caused by gross negligence, is cause for disciplinary action up to and including dismissal.