



Video Surveillance Policy

1. Purpose

This Video Surveillance Policy is designed to govern the use of Video Surveillance Systems (VSS) to enhance safety and security in Township facilities and to protect the public, employees and Township assets in accordance with the privacy provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), the Information and Privacy Commissioner (IPC) Guidelines for the Use of Video Surveillance 2015 (IPC Guidelines), and any other relevant legislation.

The policy aims to guide the use of video surveillance systems in such ways to enhance the safety and security of the public, employees and corporate assets, prevent unauthorized activities on, or involving Township property, and reduce the risk and liability exposures while ensuring compliance with MFIPPA and other applicable legislation. Section 28(1) of MFIPPA provides that personal information may be collected without consent when it is expressly authorized by statute, used for the purpose of law enforcement, or necessary for the proper administration of lawfully authorized activities.

2. Policy Scope:

This Policy applies to all Video Surveillance Systems in the care and control of the Township that is present at Township owned or leased properties and facilities. It also applies to employees including full-time, part-time, casual, contract, volunteer and co-op placements as well as contractors and service providers while performing authorized activities for the Township.

This Policy applies to the collection, use, disclosure and disposal of information collected through video surveillance technology, which is used to enhance the protection and safety of employees and the general public, reduce, deter and investigate incidents of vandalism or criminal activity, and protect Township employees, property and assets.

This Policy does not apply to video or audio recordings of Council or Committee meetings, virtual meetings that are recorded, the use of body worn cameras and does not apply to covert surveillance used as part of an investigation tool for Township by-law or other law enforcement purposes, or to workplace surveillance systems used to conduct surveillance of employees or equipment specified in the Township of Southgate Electronic Monitoring Policy.

3. Objectives:

The objectives of this policy are to govern the requirements and responsibilities with respect to:

- Compliance with Ontario's privacy laws including its obligation with respect to notice, collection, access and use, disclosure, retention and a disposal of personal information including fundamental data minimization.
- The installation and operation of video surveillance systems.



4. Definitions

- a. "CAO" means the Chief Administrative Officer of the Township of Southgate or designate.
- b. "Clerk" means the Clerk of the Township of Southgate or designate.
- c. "Consistent Purpose" means personal information collected by the Township of Southgate used for the purpose for which it was collected.
- d. "Designated Site Manager" means the manager responsible for the specific Township facility.
- e. "Facility" means any building, property or land that is either owned or occupied by the Township of Southgate.
- f. "Incident" means events or allegations of inappropriate behaviour which would be in violation of the law, or of a by-law policy or procedure relation to employee or public conduct.
- g. "MFIPPA" means the Municipal Freedom of Information and Protection of Privacy Act.
- h. "Personal Information" is defined in Section 2 of MFIPPA, as recorded information about an identifiable individual, which includes but is not limited to, information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual. If a video surveillance system displays these characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered "personal information".
- i. "Privacy Breach" means an incident involving unauthorized disclosure of personal information, including it being stole, lost or accessed by an unauthorized person.
- j. "Records Retention By-law" means the Records Retention By-law of the Township.
- k. "Video Surveillance Record" means a record of video surveillance information created from the Township's video surveillance system.
- l. "Video Surveillance System (VSS)" means a video, physical or other mechanical, electronic, digital or wireless surveillance system or device that enables continuous or periodic video recording, observing or monitoring of individuals in public spaces or within Township facilities.

5. General Provisions:

5.1 Video Surveillance Systems (VSS)

- a) The location of all video surveillance cameras and the accompanying signage must be approved by the Township CAO, Clerk, and the Designated Site Manager.
- b) Prior to the installation of VSS, the following factors must be considered:



- a. The use of VSS must be justified based on verifiable, specific reports of incidents of crime or significant safety concerns.
- b. VSS should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable.
- c. The proposed design and operation of the VSS should minimize privacy intrusion.
- d. The equipment shall not have sound capabilities unless deemed necessary for specific law enforcement purposes.
- c) Camera placement will be assessed and determined on a case-by-case basis. A Video Surveillance Security Threat Assessment shall be conducted to determine the effects the VSS may have on personal privacy and the ways in which any adverse effects can be mitigated.
- d) The VSS shall be installed to monitor only those public areas as identified requiring video surveillance.
- e) All reasonable steps shall be taken to mitigate any adverse privacy effects. No camera will be placed so that it views into an area where the public and employees have a greater expectation of privacy, such as washrooms, change rooms or directed to look through the windows of adjacent buildings or onto adjacent property.
- f) Cameras adjustable by designated employees/contractor employees should be restricted, if possible, so designated employees/contractor employees cannot adjust or manipulate the cameras to overlook spaces that are not identified or intended to be covered by the VSS system.
- g) VSS will not be used passively for surveillance purposes (meaning the equipment will not be panned or zoomed remotely) to prohibit the viewing of locations not intended to be monitored.
- h) Appropriate areas for VSS include entrances, exists, general purpose areas, common areas, corridors, receiving areas, parking lots and exterior building perimeters.
- i) The equipment may operate on a 24/7 hours and days basis.
- j) The location and particulars of the capabilities of the VSS shall be tracked and documented in the Video Surveillance Camera Location Inventory Form.
- k) All VSS storage devices shall be secure and equipped with encryption or other security measures to protect data integrity. Each storage device shall be identified by location.

6. Operation of Video Surveillance Systems:

- a) The designated site manager and employees and contractors authorized by the CAO or Clerk shall be permitted access to monitor and operate the VSS. The Clerk shall maintain an up-to-date list of all designated positions and persons.
- b) Video monitors shall only be accessed by designated employees/contracted employees. They shall be kept in a strictly controlled access area, and the monitors shall not be in a position that enables public viewing or viewing by unauthorized employees. The monitors shall be turned off when not required.

7. Public Notice:



Public Notice shall be provided to individuals that video surveillance is in use by:

- a) Posting signs, clearly visible to employees and the public, at all entrances and within common areas and/or prominently displayed on the perimeter of the grounds of all facilities under security surveillance.
- b) Informing individuals of the legal authority of the collection of personal information, the principal purpose(s) for which the personal information is intended to be used, the title, business address, and telephone number of the employee or designate who can answer questions about the collection.
- c) The public notice and sign shall be clear, and language-neutral along with a graphic depiction of the use of video security.
- d) Posting on the Township's website.

8. Use of Video Recordings:

8.1 The information collected through video surveillance shall only be used:

- a) To assess the effectiveness of safety and security measures taken at a particular facility;
- b) To investigate an incident involving the safety or security of individuals, employees, facilities or assets;
- c) To provide law enforcement agencies with evidence related to an incident under investigation;
- d) To provide evidence as require protecting the Township's legal rights;
- e) To respond to a request for information under MFIPPA;
- f) To investigate a critical bodily injury, as designated by and reported to the Ministry of Labour;
- g) To investigate an incident or allegation of serious employee misconduct;
- h) To aid in the investigation of a potential or active insurance claim;
- i) To aid in investigations of acts of vandalism or suspicious activity at Township facilities;
- j) Training; or
- k) For a consistent purpose or as required by law.

8.2 Any uncertainty whether a use is consistent with the uses outlined in this policy shall be determined by the Clerk.

8.3 Any time a Township incident report is completed indicating that the incident took place in view of a Township of Southgate Video Surveillance System, the applicable video surveillance record shall be proactively pulled and generally retained for thirty (30) days and may be disposed of thereafter if not required for a permitted use under Section 8.4(1) of this policy.

9. Access and Disclosure:



9.1 Right of Access

Any employee or member of the public who has been recorded by the VSS has a general right of access to their own personal information under Section 36 of MFIPPA and shall file a Freedom of Information (FOI) request with the Clerk.

Access to an individual's own personal information may depend upon whether third parties may be affected by the request for access and whether any exempt information may be severed from the record.

9.2 Public Requests

Any person may submit a written request for access to video surveillance records to the Clerk under MFIPPA, through the Freedom of Information (FOI) process and pay the prescribed fees.

The FOI request should contain sufficient detail, such as the approximate time and date, the location of the incident, if known, to enable an experienced employee, upon a reasonable effort, to identify the record. Access depends on whether there is an unjustified invasion of another individual's privacy and whether any exempt information can be reasonably severed from the record.

9.3 Internal Requests

Employees or authorized contractors/contractor employees/consultants shall submit a request, in writing, to the Clerk for a copy of the video surveillance footage if it is necessary in the performance of their duties and in the discharge of the Township's business, or to direct video surveillance to law enforcement. The Clerk shall determine whether access can be granted and may consult with the CAO, Human Resources and/or other persons.

9.4 Law Enforcement Requests

If access to video surveillance records is required for the purpose of law enforcement investigations, the requesting officer must complete the Law Enforcement Request Form and submit the form to the Clerk. The Clerk shall access the requested records with the assistance of the designated employee. The Clerk shall then provide the video records according to the request or pursuant to a warrant (Section 32(e) and (f) of MFIPPA).

Video surveillance records may be disclosed when staff observe illegal activity occurring on municipal property and provide the recorded footage to a law enforcement agency to support an investigation where legal proceedings may result. (Section 32(g) of MFIPPA).

Disclosure of video surveillance records may be permitted in response to a verbal request by a law enforcement agency only in situations involving an emergency, imminent danger or in hot pursuit, and under compelling circumstances affecting the health and safety of an individual.



9.5 The Clerk shall access the requested footage with the assistance of the designated employee. The Clerk shall receive the footage and provide the video records according to the request or pursuant to a warrant (Section 32(e) and (f) of MFIPPA.)

9.6. Access and Access Log Record

After any access to the VSS, the Clerk shall complete the Access Log Record.

9.7 For audit purposes, the Clerk shall log the following information in the Access Log Record:

- a) the date and time of the original, recorded incident, including the location/number of the applicable camera
- b) the name of the designated employee at the time of the incident
- c) the case file number of the agency's investigation
- d) a description of the circumstances justifying the disclosure
- e) the means used to disclose the video surveillance record.

9.8 Viewing Images

When video surveillance records must be viewed by law enforcement for investigative reasons, this must only be completed by a designated individual(s) authorized by the Clerk in a private, controlled area that is not accessible to other employees, visitors or the public.

9.9 Unauthorized Access and/or Disclosure (Privacy Breach)

If video surveillance records containing personal information are improperly disclosed or are suspected to have been disclosed to an unauthorized person and/or a potential privacy breach has occurred, the employee or contractor who is aware of the disclosure, must immediately notify the Clerk who shall follow the Privacy Protocol: Guidelines of Managing a Privacy Breach.

9.10 Access and Secure Storage

a) If the Township can redact or remove personal information of individual(s) that may have been captured on the VSS and it is considered exempt information, the Township may use tools and techniques such as:

- digitizing analogue footage to enable the use of more powerful editing tools
- blacking out or blurring images of individuals that are not subject to the request
- if the Township does not have the ability to redact or remove personal information, the Township shall outsource the requirement to a suitable provider with the consent of the request, and the cost shall be borne by the requestor.



- b) Video surveillance equipment and video surveillance records shall be stored in a secure, access-controlled location to ensure the integrity of the information.
- c) access to video surveillance records and equipment shall be limited to the Clerk and designated managers and employees.
- d) any employee accessing video surveillance records must sign a confidentiality agreement, agreeing to adhere to this policy.
- e) in accordance with the Township's Record Retention By-law, the VSS and video surveillance records shall be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved.

9.11 Retention and Destruction

- a) Brief retention periods minimize the risk of improper use or disclosure of video surveillance records. Unless the records are requested by a member of the public, an employee, or a law enforcement agency, they will be retained for up to thirty (30) calendar days. After this period, the records are considered transitory and are automatically erased through overwriting.
- b) If a video surveillance record is proactively pulled in anticipation of a request, the video surveillance record may be stored for up to thirty (30) calendar days. If a request is not received within this time, then the video surveillance record shall be manually deleted.
- c) Digital recording equipment may only be destroyed when replaced by a new piece of equipment or when it is not repairable. It may only be destroyed by an authorized service person, and it shall be destroyed in a manner that ensures that it can no longer be used by any person and that the recorded information cannot be reconstructed or retrieved by any person.
- d) When video surveillance records related to personal information have been "used", meaning when video surveillance containing images of individuals or other identifiable information is accessed or disclosed, the video surveillance records shall be retained for a period of at least one year. Simply viewing a live feed does not represent a "use" of personal information.

9.12 Training

Employees and contractors who have access to the VSS equipment and the video surveillance records shall receive training in accordance with the provisions of this policy. Training will be carried out by the Clerk using the Video Surveillance Policy Training Checklist.

9.13 Regular Audit and Evaluation

The Clerk shall conduct regular reviews of the VSS and this policy to ensure that:



- Video surveillance continues to be justified according to the camera inventory and if so, whether its use can be restricted.
- Reported incidents and access pursuant to a request is properly recorded in the access log.
- Video surveillance records are being properly retained and/or destroyed; and
- Any formal or information requests from the public have been tracked.

9.14 Delegation of Authority

After approval of this policy, the Clerk is hereby delegated the authority to amend this policy from time to time as deemed necessary.

10. Roles and Responsibilities

10.1 Chief Administrative Officer shall:

- Ensure consistent application and Township wide compliance with this policy.

10.2 The Clerk shall:

- Process requests for disclosure of video surveillance records under MFIPPA
- Respond to requests from the public and employees about the collection, use and disclosure of personal information captured by the VSS.
- Provide advice and recommendations to employees to assist in complying with this policy and MFIPPA.
- Facilitate access requests by law enforcement agencies.
- Post the VSS Notice of Collection of Personal Information on the Township's website.
- Work with department manager(s) and employee(s) in the event of an improper disclosure of personal information.
- Notify the IPC in the event of a privacy breach, where appropriate.

10.3 The Designated Site Manager shall:

- Be responsible for the overall management of the video surveillance program at their designated site.
- Ensure a public notice for video surveillance is posted at Township sites that have a VSS camera at their designated site notifying the public of the collection of personal information and the use of the information.
- Provide job specific training.
- Ensure those employees designated to be responsible for the VSS operations at their site comply with this policy and related directions, including:
 - Complying and adhering to all aspects of this policy.
 - Monitoring the video surveillance cameras.
 - Ensuring all aspects of the VSS are functioning properly.
 - Documenting all relevant information as directed by the Clerk.



- Ensuring that no personal information is disclosed without approval of the Clerk.
- Ensuring that no copies of video surveillance records, data/images, in any format are taken from the VSS without the approval of the Clerk.
- Forwarding all requests for access to video surveillance records to the Township for properties.

10.4 The Clerk and the Designated Site Manager shall jointly:

- Ensure the reasons for the proposed video surveillance equipment/systems are consistent with the IPC Guidelines for the use of video surveillance cameras in public places.
- Undertake regular evaluations of the VSS to ensure compliance with this policy and to ensure the camera locations are still necessary.
- Approve all camera locations.
- Develop VSS and privacy training for Township and contract staff who have responsibilities under this policy.
- Conduct internal audits of the system, as required to ensure compliance with this policy and MFIPPA.

10.5 All Employees Shall

- Review and comply with this policy and MFIPPA in performing their duties and responsibilities related to the operation of the VSS.
- Report any suspected privacy breach to their manager or supervisor.
- Report any problems with the VSS to their managers or supervisors.

10.6 Where the Township has a contract with a service provider, the contract shall provide that failure by the service provider to comply with relevant legislation, and established policies and procedures is considered a breach of contract leading to penalties and including contract termination.

11. References:

- [The IPC Guideline for the Use of Video Surveillance](#) – October 2015 and future updates
- [IPC Technology Fact Sheet – Video Surveillance](#) – November 2016
- [The Municipal Freedom of Information and Protection of Privacy Act](#)
- [The Municipal Act](#)
- [Township of Southgate Policy No. 93 – Electronic Monitoring Policy](#)
- [By-law 2017-036 – Records Retention By-law](#)

12. Policy Review Cycle

This policy will be reviewed at minimum every three (3) years and updated if required.

Video Surveillance Camera Location Inventory

[illegible]



ATTENTION

This Area is Monitored by Video Surveillance Cameras

The personal information collected using the CCTV at this site is collected under the authority of the Municipal Freedom of Information and Protection of Privacy Act.

This information is used for the purpose of promoting public safety and the prevention and reduction of incidents/crime at this site.

Any questions, about this collection of personal information can be directed to the Township of Southgate Clerk at 185667 Grey Road 9, Dundalk, On, N0C 1B0



Law Enforcement Officer Request Form – Access to Video Surveillance

The following information is being requested under Section 32(g) of the Municipal Freedom of Information and Protection of Privacy Act which provides for the disclosure of records containing personal information of an individual for the purpose of aiding an investigation with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

Part One: Details of Request (to be completed by the Law Enforcement Officer)

Department/Division which holds the information (if known):	Name of Law Enforcement Agency:	Name of Law Enforcement Officer and Badge/ID Number:
The following records are requested: 1. 2. 3. 4.		
Containing the personal information of _____ (list names 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, or there is a reasonable basis to believe that an offence may have been committed, and the disclosure is to enable the law enforcement agency to conduct such an investigation. Initial Here:		
Occurrence/Investigation Number:	Telephone (Requesting Officer): Email Address:	Signature of Officer: Date:

TOWNSHIP OF SOUTHGATE
Policy # 104
Video Surveillance Policy
Council Approval: August 5, 2026



Will the video surveillance record be returned to the Township? _____			
Will the video surveillance records be securely destroyed by the Agency? _____			
Review Original Records (yes or no): _____			
Copies Request (yes or no): _____			
For Office Use Only:		File #	
Part Two – Access Log Record	Records Disclosed (to be completed by Township employee disclosing records)	For internal use only	
Department/Division	Employee Name:	Title/Position:	Telephone:
Video Surveillance Records Disclosed (describe records disclosed including format (downloaded to a shared drive and emailed, print, thumb drive, etc):			

Please ensure that a copy of the disclosed record is saved in the Township's electronic record filing system. When video surveillance records containing personal information has been used (accessed or disclosed) the video surveillance records must be retained for at least one year.

 Signature of Employee

 Date

Personal information contained in this form is collected pursuant to the Municipal Freedom of Information and Protection Act and will be used in accordance with the Township Video Surveillance Policy. Questions about the collection should be directed to the Clerk of the Township of Southgate.



Internal Request Form for Disclosure of Video Surveillance Records

Using this form, employees or authorized contractors/consultants/agenda/insurance adjusters may request a copy of video surveillance records if it is necessary in the performance of their duties and is in the discharge of the Township's business. The completed form shall be submitted to the Township Clerk/designate either by hand delivery or via confidential email.

The Clerk/designate shall determine whether access can be provided. In deciding, the Clerk may consult with Human Resources and/or other persons.

Name of Employee: _____ Department: _____

Cell Number or Extension _____ Email: _____

OR

Name of Employee or Authorized Contractor/Consultant/Agent/Insurance Adjuster (please indicate appropriate entity): _____

Name of authorized Contractor/Consultant/Agent/Insurance Adjuster:

The following records are requested:

1. _____

2. _____

3. _____

4. _____

Containing the personal information of: _____

I, the undersigned, confirm that access to the video surveillance records is necessary in the performance of my duties and in the discharge of the Township's business **for the following reasons:**

TOWNSHIP OF SOUTHGATE
Policy # 104
Video Surveillance Policy
Council Approval: August 5, 2026



I understand the Clerk/designate and operator shall retrieve the footage and provide it to the appropriate law enforcement agency or other competent authority. The Clerk/designate may determine whether the employee/contractor requires access to the video surveillance records and length of time.

Signature of Employee

Date

For Office Use Only:		File #
Department/Division:	Employee Name:	Title/Position:
Consultation (Please circle if applicable)		
Human Resources	Legal Opinion	Other: _____
Describe Video Records Disclosed (including format of records, i.e shared drive, link, thumb drive, print etc.):		
Signature of Clerk/Designate:		Date:

Personal information contained in this form is collected pursuant to the Municipal Freedom of Information and Protection of Privacy Act and will be used in accordance with the Township of Southgate's Video Surveillance Policy. Questions about this collection may be directed to the Clerk of the Township of Southgate.



Video Surveillance Records Access Log Form

Please complete this form each time a video surveillance record is accessed by an employee/contractor of the Township of Southgate and/or released pursuant to a written request by an individual, employee or a law enforcement agency (including an emergency verbal request by law enforcement) in accordance with the Video Surveillance Policy.

This form shall be filed with the Township Clerk or designate.

Employee Name and Title	Phone Number/Ext./Email Address	File Number:

Name of operator at the time of incident: _____

Footage Accessed – Camera # and Location	Date and Time of Recording	Name of employee/contractor or accessing footage	Date and time when footage accessed	Reason for accessing footage (i.e. investigation, audit, routine check)	Method of Access (on-site or remotely)	Name of Person/Title reviewing the access log form	Notes (any additional information)

Please ensure that the video footage will be sent to the Clerk's department and will be retained for at least one year.



Video Surveillance Confidentiality Agreement

I, _____ (name of employee) declare I am an employee of the Township of Southgate, who may from time to time, be requested to monitor and access video surveillance recordings as set out in the Video Surveillance Policy of the Township of Southgate.

OR

I, _____ (name of employee/contractor) declare I am an employee of _____ (name of contractor) who may from time to time, be requested to monitor and access video surveillance recordings as set out in the Video Surveillance Policy of the Township of Southgate.

I hereby acknowledge, understand and agree that:

1. I have read and understand the Video Surveillance Policy of the Township of Southgate ("Policy").
2. I shall comply with the provisions of the Policy.
3. I will ensure all reasonable precautions are taken to protect the personal information collected by the video surveillance system as required by the Municipal Freedom of Information and Protection of Privacy Act and the Policy, and I will not disclose any information to any unauthorized person(s).
4. I will keep the recordings, data and information always collected by the video surveillance system confidential and I will ensure access to such information is strictly controlled as set out in the Policy.
5. I will not publicize, divulge or release any information collected by the video surveillance system except to, or with the prior written consent of the Clerk or designate.
6. I will only access the personal information collected by the video surveillance system except to, or with the prior written consent of the Township Clerk or designate.
7. I will not make copies of any recordings or data in any format, including electronic formats, unless I receive written or explicit approval from the Township Clerk.
8. I will adhere to this Policy, and I will not access or use information contained in the video surveillance system, its components, files or database for personal reasons, nor dispose, destroy, erase or alter any record without proper authorization and without following the requirements contained in the Policy.
9. All recordings, data and information related to the video surveillance system shall remain the exclusive property of the Township of Southgate.

TOWNSHIP OF SOUTHGATE
Policy # 104
Video Surveillance Policy
Council Approval: August 5, 2026



10. I will immediately notify the Clerk or designate, if I receive notice that I may, or will, be legally required to disclose video recordings. Prior to disclosing any video surveillance information, the Clerk must be consulted so that, if necessary, they can attempt to prevent or limit such disclosure.

11. Any breach of confidentiality of the recordings, data and information collected by the video surveillance system could result in disciplinary measures, including dismissal from my employment (or cancellation of the contract with the Township of Southgate.)

Agreed and accepted this _____ day of _____, 202__.

Employee Name

Date

Manager/Supervisor Signature

Date

Upon completion of the confidentiality agreement, please deliver the original to the Clerk's office for retention.



Video Surveillance Policy Training Checklist

Employee or Contractor Employee Name:
Division/Section or Company:
Position Title:

General Statement

The information and Privacy Commissioner of Ontario "Guidelines for Video Surveillance Cameras in Public Places" forms the basis for the Township of Southgate's Video Surveillance Policy. The guidelines that that a Video Surveillance Policy should include "... the incorporation of the policy into training and orientation programs of an institution and service provider" and that the "...training programs addressing staff obligations under the Act should be conducted on a regular basis."

The Township of Southgate intends to meet its training obligations using the Training Checklist and formal training.

1. Policies and Procedures

#	Question	Yes	No	Comments
A	I have received a copy of, read and understand the Township of Southgate Video Surveillance Policy, the applicable appendices and forms.			
B	I have received a copy of, read and understand the Privacy Breach Protocol and Guidelines.			

2. Roles and Responsibilities

#	Question	Yes	No	Comments
A	I understand the roles and responsibilities of the Clerk, Designate Site Manager and designated employees/contractor employees.			
B	I understand and will carry out the duties and responsibilities of the designated employees/contractor employees, if applicable.			



3. Guidelines for the Implementation of a Video Surveillance Policy

#	Question	Yes	No	Comments
A	I am aware the video surveillance equipment should only be installed and used to monitor those spaces that have been identified as requiring video surveillance.			
B	I am aware that no person shall adjust or manipulate cameras to overlook spaces that are not intended to be covered by the video surveillance system.			
C	I am aware that equipment should never be used to monitor the inside of areas where the public and employees have a higher expectation of privacy (i.e. washrooms, changing rooms, etc.).			
D	I am aware that all video surveillance installations must be clearly marked to advise staff and members of the public that the video surveillance is in use.			
E	I am aware that signs shall be posted at all entrances and/or on the perimeter of the property under surveillance.			

4. Video Surveillance Equipment/Records

#	Question	Yes	No	Comments
A	I am aware that each designated employee/contractor employee shall maintain a logbook to record all activities related to video surveillance, including use, maintenance and storage of video surveillance records and that each entry shall include the name of authorized staff, date, time and activity.			
B	I am aware that designated employees/contractor employees must document all information regarding the use, maintenance and storage of records in the logbook, including all instances of access to and use of, recorded material to enable a proper audit trail.			
C	I am aware that designated employees/contract employees shall			

TOWNSHIP OF SOUTHGATE
Policy # 104
Video Surveillance Policy
Council Approval: August 5, 2026



	not deliberately enter false or incomplete information or delete existing information in any logbook and may not take any unauthorized action that would cause the destruction or alteration of any information contained in the logbook.			
D	I am aware that designated employees/contractor employees shall not make any changes to the identification or labels of records either in hardcopy or electronic format.			
E	I am aware that all storage devices and hard drives that are not in use must be securely stored and located in an access-controlled area.			
F	I am aware that designated employees/contractors employees shall not make any copies of data/images in any format (hardcopy/electronic, etc.) from the video surveillance system without the approval of the Designated Site Manager or Clerk, following the protocols set out in the Video Surveillance Policy.			

5. Access to Video Surveillance Records

#	Question	Yes	No	Comments
A	I am aware that designated employees/contractor employees may access information only when necessary to perform work as assigned to accomplish the business of the Township.			
B	I am aware that designated employees/contractor employees must not access or use information from any component(s) of the video surveillance system files or database for personal reasons.			
C	I am aware that access to the video surveillance records created by the video surveillance system, including logbooks and audit trails, shall be restricted to authorized personnel only.			
D	I am aware that designated employees/contractor employees shall not disclose personal information and that disclosure should only occur by the said employee in consultation, as necessary with the clerk to ensure the			

TOWNSHIP OF SOUTHGATE
Policy # 104
Video Surveillance Policy
Council Approval: August 5, 2026



	information is being disclosed in accordance with the <i>Municipal Freedom of Information and Protection of Privacy Act</i> .			
E	I am aware of and understand the Freedom of Information (FOI) Formal Access Request process.			
F	I am aware of and understand the Formal Access Request process and forms for Law Enforcement Agencies and for internal use.			

6. Viewing Images

#	Question	Yes	No	Comments
A	I understand that video surveillance monitors shall be concealed from the public and unauthorized employees (monitors shall not be public facing).			
B	I understand when recorded images from the camera must be viewed for law enforcement investigative reasons it shall be done in a private, controlled area that is not accessible to other employees and/or visitors.			

7. Retention and Disposal of Records

#	Question	Yes	No	Comments
A	I am aware that a designated employee/contractor employee must not disperse, destroy or erase any video surveillance record without proper authorization and without following the provisions of the Video Surveillance Policy.			
B	I understand video surveillance records will only be retained for no more than 30 days.			
C	I am aware that requests by Law Enforcement Agencies for copies of video surveillance recordings specific to a reported incident/investigation will be retained for at least one year.			
D	I understand the designated employee/contractor employee shall take all reasonable efforts to ensure the security of records in the Township's custody and control.			
E	I understand that all storage devices must be disposed of in accordance with the Video Surveillance Policy ensuring			

TOWNSHIP OF SOUTHGATE
Policy # 104
Video Surveillance Policy
Council Approval: August 5, 2026



	personal information is erased, shredded, or burned and cannot be retrieved or reconstructed.			
--	---	--	--	--

8. Unauthorized Access and/or Disclosure

#	Question	Yes	No	Comments
A	I understand that any designated employee/contractor employees and/or Township employee who becomes aware of any unauthorized disclosure of a video surveillance record in contravention of the Video Surveillance Policy and/or a potential privacy breach are to immediately notify the Clerk			
B	I understand that intentional wrongful disclosure, or disclosure caused by negligence by the Township's employees may result in disciplinary action up to and including dismissal. Intentional wrongful disclosure, or disclosure caused by negligence, by contractor to the Township, may result in termination of their contract.			

9. Inquiries from the Public

#	Question	Yes	No	Comments
A	I am aware that any designated employee receiving an inquiry from the public regarding the Video Surveillance Policy shall direct to the inquiry to the Clerk by email to clerks@southgate.ca			

10. Audit

#	Question	Yes	No	Comments
A	I am aware that the Clerk and Designated Site Manager may designate employees to conduct random site visits or audit compliance with the Video Surveillance Policy.			

I, _____, hereby confirm that I have completed the Video Surveillance Policy training provided by the Township of Southgate.

Name of Employee/Contractor

Signature

Date

Name of Trainer

Signature

Date



Privacy Breach Protocol: Guidelines for Managing a Privacy Breach

Introduction:

What is a privacy breach?

A privacy breach occurs when personal information is collected, used, disclosed and/or destroyed in ways that are not in accordance with the privacy provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (the Act).

The most common breach of personal information is unauthorized disclosure of personal information contrary to Section 32 of the Act. Types of breaches include:

- A lost or misplaced file
- A lost or stolen laptop
- Unauthorized access to personal information (electronic/hardcopy); or
- The inadvertent disclosure of personal information (e.g. human error in misdirecting an email or leaving sensitive information on a desk)

Potential Privacy Breach Actions

When faced with a privacy breach, take the following actions immediately:

Identify the scope of the potential breach and take steps to contain it:

- Ensure appropriate staff within the Township are immediately notified, including the Clerk/designate, the appropriate Department Manager and the CAO.
- Immediately isolate any physical or system resource that may contain evidence (e.g. paper files, workstations, logs, electronic records, email files, etc.)
- Keep existing back-ups and back up any system resource associated with the incident.
- Retrieve the hard copies of any personal information disclosed.
- Ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive information and obtain the individual's contact information if follow-up is required.
- In consultation with the appropriate staff, determine whether the privacy breach could allow unauthorized access to any other personal information.
- Document all actions (dates and times) taken during containment.
- Determine if the response to the incident needs to be escalated (e.g. by telephone or in writing).

Notify Affected Person(s) of Privacy Breach

- Identify those individuals who privacy was breached and, barring exceptional circumstances (e.g. no known last address), notify those individual (e.g. by telephone or in writing)



- Provide details of the extent of the breach and the specifics of personal information at issue and advice of the steps that have been taken to address the breach, both immediate and long-term.

Investigate the Privacy Breach

- The Clerk or designate shall inform the Information and Privacy Commissioner of Ontario (OPC) Registrar of the privacy breach and advise of immediate containment and notification actions taken by the Township.
- The Clerk or designate in consultation with the IPC and department staff shall conduct an internal investigation into the matter:
 - The objectives of the investigation are to ensure immediate requirements of containment and notification have been addressed
 - Review the circumstances surrounding the breach
 - Review the adequacy of existing policies and procedures in protecting personal information and implement changes to prevent future breaches.
 - Program-wide or institution-wide procedures may warrant a review (e.g. incidents such as a misdirected email or inadequate system access controls).
- The Clerk shall advise the IPC in writing of the Township's findings and work together with departmental staff and the IPC to make any necessary changes. The IPC may issue a report with recommendations

Resolutions/Remedies

- Implement IPC recommendations (e.g. revising and/or redeveloping policies and procedures)
- Ensure staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of the Act.

Conclusion

These guidelines have been prepared by the Clerk's Office and are intended to provide more basic information on how to proceed in the event of a privacy breach. For more information, please contact the Clerk at clerks@southgate.ca.



Video Surveillance Threat Assessment
To Determine Requirements for a Video Surveillance System

Section 1 – Facility Information

Name of Facility: _____
Address of Facility: _____
Name of Requester: _____ Department: _____
Proposed Video Location: _____

Section 2 – Existing Video Surveillance

Does a video surveillance camera(s) currently exist at this facility?

No: _____
Yes: _____

If yes, please describe the location and if the set-up adheres to the Township of Southgate Video Surveillance Policy.

Section 3 – Documentation for Safety Concern

The use of each video surveillance camera should be justified based on verifiable specific reports of incidents of crime or significant safety concerns. Are there any documented incidents of crime or significant safety concerns in any of the following formats?

#3	Documentation Forms	Yes	No	Comments
A	Security Occurrence History/Reports			
B	Police Reports			
C	H&S Concerns			
D	Other			

Score 1 Point for "Yes"
Subtotal Score (out of 4): _____



Section 4 – Privacy Impact Mitigation

An assessment should be conducted of the efforts of the property video surveillance camera(s) may have on personal privacy and how adverse effects can be mitigated. Have the following effects and mitigation strategies been considered?

#4	Documentation Forms	Yes	No	Comments
A	The location of the proposed camera is situated in an area that will minimize privacy intrusion.			
B	Does the proposed camera location impact on the public/employee's higher expectation of privacy (i.e not in a washroom, or change room, etc.)			
C	Is the location of the proposed camera visible?			
D	Can the video surveillance be restricted to the recognized problem area?			
E	Is the space allocated for proper video surveillance signage?			
F	Have drawings been attached showing the video location?			
G	Other			

Score 2 Point for Each "Yes"
Subtotal Score (Out of 12): _____

Section 6 – Operational Safeguards

The proposed design and operation of the video surveillance system should minimize privacy intrusion. Have the following design and operation factors been considered for each proposed camera location?

#5	Measures to Mitigate Effects	Yes	No	Comments
A	Can the proposed camera be restricted to ensure			



	Operators cannot adjust or manipulate cameras to overlook spaces that a threat assessment has not been undertaken?			
B	If applicable, is the video surveillance monitor intended to be in an area with strictly controlled access?			
C	Will the video surveillance monitor be situated so that it will be hidden from public view?			
D	Other			

Score 1 Point for Each "Yes"

Subtotal Score (Out of 4): _____

Section 7 – Final Score and Ranking

Total Score (Out of 12): _____

Priority Ranking:

High (14-20 Points): Strong case for surveillance, proceed with planning.

Medium (6-13 Points): Consider alternative mitigations or limited implementation

Low (0-5 Points): Reassess need or focus on non-surveillance solutions.

Section 8 – Additional Comments
