

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
--	--------------	---------

Appendix “A”

Effective as of _____

1.0 Purpose

- 1.1 The Municipality recognizes the need to balance an individual’s right to privacy and the need to ensure the safety and security of the Municipality’s staff, clients, visitors, and property. While video surveillance cameras are installed for safety and security reasons, the Municipality’s video surveillance systems 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 municipal facilities and properties operating in a safe, secure, and privacy protective manner.
- 1.2 Video security surveillance systems are a resource used by the Municipality for the purpose of increasing the safety and security of staff and members of the public, to protect public safety, corporate assets, and property, and to detect and deter criminal activity and vandalism.
- 1.3 The Municipality is authorized to conduct video surveillance under Section 28(2) of the *Municipal Freedom of Information and Protection of Privacy Act* (“*MFIPPA*”). The Municipality recognizes that video surveillance technology has the potential for infringing upon an individual’s right to privacy and although video surveillance technology may be required for legitimate operational purposes, its use must be in accordance with the provisions of *MFIPPA* and any other applicable privacy laws.
- 1.4 This policy does not require or guarantee that a camera or recording equipment will be recording or monitored at all times.

2.0 Scope

- 2.1 This policy applies to all types of camera surveillance systems, surveillance monitors, and camera recording devices used by the Municipality, notwithstanding the following exceptions: red light cameras, dash cams, cameras owned by the Chatham-Kent Police Services, built-in webcams on end-user devices such as laptops, tablets, and cell phones, or any surveillance system for which there is an alternative corporate- approved policy.
- 2.2 This policy applies to all municipal Employees and Service Providers involved in the operation of this video surveillance program. These employees have been trained on this policy and their statutory obligations in performing their duties and functions related to the operation of the video surveillance system and the video surveillance program and may be subject to discipline if they breach this policy or applicable privacy laws.

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

3.0 Definitions

3.1 For the purpose of this policy, the following definitions apply:

Legal Framework

In protecting the privacy of Personal Information, the following different pieces of legislation regulate the collection, use and disclosure of Personal Information for the Municipality:

- ☒ *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* controls the collection and use of Personal Information held by Ontario Municipalities, including the Municipality of Chatham-Kent and certain designated organizations.
- ☒ *Fixing Long-Term Care Act*, where applicable.
- ☒ *Personal Health Information Protection Act (PHIPA)*, where applicable.
- ☒ *Personal Information Protection and Electronic Documents Act (PIPEDA)*, where applicable.

Employee

An “employee” is defined in this policy as someone who is working for the Municipality of Chatham-Kent. All employees shall comply with this policy and all applicable privacy legislation as it relates to their particular employment responsibilities.

Personal Information

Personal Information as collected by the Municipality pursuant to this policy means recorded information about an identifiable individual, including, but not limited to, information relating to an individual’s race, colour, national or ethnic origin, sex and age. If a video surveillance system displays such characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered Personal Information.

Service Provider

The term Service Provider shall include but is not limited to any contractor, agent, household worker, tradesperson, or other person hired by the Municipality of Chatham-Kent to provide a service or product. All Service Providers shall comply with this policy and all applicable privacy legislation as it relates to their particular employment and/or contractual responsibilities.

4.0 Roles and Responsibilities

4.1 Directors

A Director may delegate various responsibilities to members of its department under this policy. The key duties of each Director include:

- a) Ensuring compliance for Employees and Service Providers who have

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

- responsibilities under this policy;
- b) Undertaking evaluations of video surveillance system installations;
- c) Reviewing this policy;
- d) Receiving status updates from Facility Video Supervisors regarding staff adherence to the responsibilities within this policy;
- e) Providing advice and recommendations to staff in compliance with the Legal Framework;
- f) Receiving access requests for video surveillance records and directing access requests to the Municipal Clerk (FOI Coordinator);
- g) Responding to privacy complaints related to video installations in consultation with the Municipal Clerk;
- h) Investigating video surveillance security and any privacy breaches that occur in consultation with the Municipal Clerk;
- i) In consultation with the Facility Video Supervisors, ensuring all Operators receive training regarding obligations and compliance with the Legal Framework and this Policy.

4.2 Facility Video Supervisors

Those Employees responsible for the delivery of services within a particular facility in which a video surveillance system is installed shall be referred to as Facility Video Supervisors in this policy. For facilities where there are multiple services being delivered by different municipal departments, each department's Director shall designate a Facility Video Supervisor for the specific video surveillance system(s) at the location, as applicable. As designated by their Director, a Facility Video Supervisor shall:

- a) Conduct Security Threat Assessments to determine the requirement for a video surveillance system;
- b) Where appropriate, consult with relevant community groups who may be disproportionately impacted by the installation of video surveillance systems;
- c) Prepare recommendations for their Director for review and installation approval of video surveillance systems;
- d) Approve installation of video cameras at the facility(ies) for which they are responsible;
- e) Advise on placement of video surveillance monitoring signs;
- f) In consultation with the Municipal Clerk, provide training to all Operators regarding obligations and compliance with the applicable privacy legislation and this policy;
- g) Consult with their Director regarding all requests for access to video records and/or forward requests/complaints to the Director;
- h) Be responsible for the life-cycle management of authorized video security surveillance systems, specifications, equipment standards, installation, maintenance, replacement, disposal and related requirements (e.g. signage), including:

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

- i. Documenting the reason for implementation of a video surveillance system at the designated area;
- ii. Maintaining a policy regarding the locations of the reception equipment;
- iii. Maintaining a list of personnel who are authorized to operate the systems and access any recordings, including the circumstances under which access is permitted. Logs must be kept of any access to such recordings;
- iv. Maintaining a record of the times when video surveillance will be in effect;
- v. Assuming responsibility for the day-to-day operation of the system in accordance with policies, procedures and direction/guidance that may be issued from time-to-time, and keeping a log as noted in Appendix #2: Record Keeping Log;
- vi. Completing a five-year review for each authorized video surveillance system in their area of responsibility and advising the Director if the system needs to remain in place as-is, needs to be upgraded to newer technology to continue to serve its purpose at the location, or if the system can be removed from the location. If the recommendation is that the system be removed, justification needs to be provided to the Director as to why this is the case (e.g. a lessening of criminal activity at the specific location);
- vii. In the absence of the management staff with designated responsibilities, alternate management staff will take responsibility.

4.3 Operators

Operators are any Staff or Service Providers entrusted by a Facility Video Supervisor to operate the video surveillance system for a particular facility. The duties and responsibilities of the Operator include:

- a) Complying and adhering to all aspects of this Policy;
- b) Accessing the video surveillance camera recordings to view specific time frames if an incident comes under investigation by supervisory or management staff, or law enforcement agencies;
- c) Ensuring all aspects of the video surveillance system are functioning properly;
- d) Documenting all information regarding the use, maintenance, and storage of records in the applicable logbook, including all instances of access to, and use of, recorded material to enable a proper audit trail;
- e) Ensuring that no Personal Information is disclosed in accordance with the applicable privacy legislation and this policy;

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

- f) Ensuring that no copies of data/images in any format (hardcopy, electronic, etc.) is taken from the video surveillance system without approval from their Director or Facility Video Supervisor;
- g) Forwarding all requests for access to video records to their Director.

4.4 Employees

All Employees must adhere to this policy and must not disclose, 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 regulations contained in this policy.

4.5 Service Providers

The Municipality will ensure that any agreements between the Municipality and its Service Providers state that records under the video surveillance program remain under the Municipality's control and subject to applicable privacy laws. The following sample clause may be inserted into contracts or agreements with third party Service Providers:

While on municipal property, visitors, guests, and service providers may be recorded by video surveillance equipment installed throughout the premises. The Personal Information recorded by such equipment is the property of the Municipality and will be collected, stored, and destroyed in accordance with all appropriate provincial and federal laws and in accordance with the Municipality's Video Surveillance Policy
(_____)

Violation of this policy or applicable privacy laws by Service Providers will be considered a breach of the contract.

5.0 Guidelines to Follow Prior to the Implementation of a Video Surveillance System

5.1 Factors to Consider Prior to Using Video

Before deciding to install video surveillance, the following factors must be considered:

- a) The use of video surveillance cameras should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns;
- b) A video surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable and/or did not resolve the initiating factor(s);

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

- c) An assessment must be conducted on the effects that the proposed video surveillance system may have on personal privacy, and the ways in which any adverse effects can be mitigated;
- d) The proposed design and operation of the video surveillance systems should minimize privacy intrusion. A form has been provided to assist in reviewing these factors - See Appendix #3: Surveillance Video Security Threat Assessment.

5.2 Designing and Installing Video Surveillance Equipment

When designing a video surveillance system and installing equipment, the following must be considered:

- a) Given the open and public nature of some municipal facilities and the need to provide for the safety and security of Employees and citizens who may be present at such facilities at all hours of the day, the Municipality's video surveillance systems may operate at any time in a 24 hour period;
- b) The video equipment shall be installed to only monitor those spaces that have been identified as requiring video surveillance;
- c) Operators' ability to adjust cameras shall be restricted so that Operators cannot adjust or manipulate cameras to overlook spaces that are not intended to be covered by the video surveillance program;
- d) Equipment shall never monitor the inside of areas where the public and Employees have a higher expectation of privacy (e.g. change rooms and washrooms);
- e) Where possible, video surveillance should be restricted to periods when there is a demonstrably higher likelihood of crime being committed and detected in the area under surveillance;
- f) Reception/recording equipment must be located in a strictly controlled access area. Access to the video surveillance system and any video recordings is restricted to authorized Operators and is protected by password;
- g) Every reasonable attempt should be made by video Operators to ensure video monitors are not in a position that enables the public and/or unauthorized staff to view the monitors

5.3 Notice of Use of Video Systems

In order to provide notice to individuals that video is in use:

- a) The Municipality shall post a sign, visible to members of the public, at all entrances and/or prominently displayed on the perimeter of the grounds under video surveillance.

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

- b) The notification requirements of this sign must inform individuals of the legal authority for the collection of Personal Information; the principal purpose(s) for which the personal information is intended to be used; and the title, business address, and telephone number of someone who can answer questions about the collection - See Appendix #1: Notice of Collection.

5.4 Personnel Authorized to Operate Video Equipment

Only Operators and Service Providers designated by a Facility Video Supervisor or a Director shall be permitted to operate video surveillance systems.

6.0 Video Equipment/Records

6.1 Types of Recording Devices

The Municipality's video systems include, but are not limited to, Digital Video Recorders. Facilities using video recorders of any kind will retain these records for a maximum of 60 days. A record of an incident may be stored longer than the 60 days where it may be required as part of a criminal, safety, or security investigation or for evidentiary purposes.

6.2 Record Identification

All records (storage devices) shall be clearly identified as to the date and location of origin including being labelled with a unique, sequential number or other verifiable symbol. In facilities with a video system that stores information directly on a hard drive, the computer time and date stamp shall be understood to be this identification.

6.3 Logbook

Operators shall maintain a physical or electronic logbook to record all activities related to video devices and records. The activities include all information regarding the use, maintenance, and storage of records and all instances of access to, and use of, recorded material. All logbook entries will detail authorized staff, date, time and activity. A physical logbook must remain in a safe and secure location with the video recording equipment, and an electronic logbook must be adequately protected as per IT recommendations, in order to ensure protection of the data. Only the Facility Video Supervisors or Directors are authorized to remove a physical logbook from a secure location or change the format of an electronic logbook - See Appendix #2: Record Keeping Log.

7.0 Access to Video Records

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

7.1 Access

Access to the video surveillance records (e.g. logbook entries, CD, digital recordings, etc.) shall be restricted to authorized personnel only in order to comply with their roles and responsibilities as outlined in this Policy.

7.2 Storage

Storage devices that are not in use must be stored securely in a locked receptacle located in an access-controlled area.

7.3 Formal Access Requests Process

In accordance with *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)*, all requests for video records must be directed to the Municipal Governance division of the Municipality, specifically to the attention of the FOI Coordinator. A person requesting access to a record is required to complete Chatham-Kent's Freedom of Information and Protection of Privacy Request Form. The individual requesting the record must:

- a) Provide sufficient detail (the approximate time and date, the location - if known - of the incident, etc.) to enable an Employee of the Municipality, upon a reasonable effort, to identify the record; and
- b) At the time of making the request, pay the prescribed fees as provided for under the *Municipal Freedom of Information and Protection of Privacy Act*.

7.4 Viewing Images

When recorded images from the cameras must be viewed for law enforcement or investigative reasons, as directed by the FOI Coordinator, this must only be completed by an individual or individuals authorized by the Facility Video Supervisor in a private, controlled area that is not accessible to other staff and/or visitors.

7.5 Custody, Control, Retention and Disposal of Video Records / Recordings

The Municipality retains custody and control of all original video records not provided to law enforcement. Video records are subject to the access and privacy requirements of the *MFIPPA*, *PIPEDA*, and *PHIPA*. These requirements include, but are not limited to, prohibition of all Employees from access or use of information from the video surveillance system, as well as its components, files, and/or database for personal reasons. With the exception of records retained for criminal, safety, or security investigations or evidentiary purposes, the Municipality must not maintain a copy of recordings for longer than the recording systems' 60 day recording cycle. The Municipality will take all reasonable efforts to ensure the security of records in its control/custody and ensure their safe and secure disposal. Old storage devices must be disposed of in accordance with an applicable

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

technology asset disposal process ensuring Personal Information is erased prior to disposal, and cannot be retrieved or reconstructed. Disposal methods may include shredding, burning, or erasing depending on the type of storage device. Written disposal records will be maintained in a safe and secure location with the video recording equipment - See Appendix #2: Record Keeping Log.

Personal Information that has been viewed for law enforcement and public safety purposes must be retained for one year or a shorter retention period set out in a by-law or resolution unless the individual to whom the information relates consents to its earlier disposal (Ont. Reg. 823, s5).

7.6 Unauthorized Access and/or Disclosure (Privacy Breach)

Employees that become aware of any unauthorized disclosure of a video record in contravention of this Policy and/or a potential privacy breach are to immediately notify the Facility Video Supervisor and/or their Director. After this unauthorized disclosure or potential privacy breach is reported:

- a) The Director and Municipal Clerk shall follow any applicable municipal privacy management policies in place at the time;
- b) The Facility Video Supervisor shall inform their Director of events that have led up to the privacy breach;
- c) The staff member shall work with the Facility Video Supervisor and their Director to take all reasonable actions to recover the record and limit the record's disclosure;
- d) The Director, in consultation with the Facility Video Supervisor will notify affected parties whose Personal Information was inappropriately disclosed;
- e) The Facility Video Supervisor, in consultation with their Director, shall investigate the cause of the disclosure with the goal of eliminating potential future occurrences.

A breach of this policy by an Employee may result in discipline up to and including dismissal. A breach of this policy by Service Providers may result in termination of their contract.

8.0 Related Policies

Please refer to the following policies related to this corporate policy:

- a) Corporate IT Acceptable Use Policy
- b) Corporate IT Security Policy – Access Control

Appendix 1: Notice of Collection

--

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
--	--------------	---------

ATTENTION



These premises are subject to

VIDEO SURVEILLANCE

WARNING

Video Surveillance is not intended to be an emergency response system

IN THE EVENT OF A LIFE THREATENING EMERGENCY CALL 911

The personal information collected by the use of the Video Surveillance Cameras at this site is collected under the authority of the *Municipal Act, 2001*. This information is used for the purpose of promoting public safety and reduction of crime at this site.

Any questions about this collection can be directed to:

Municipal Clerk at 519-360-1998

315 King Street West, Chatham, ON N7M 5K8

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

Appendix 2: Record Keeping Log

Date	Time	Name of Employee (Operator)	Record ID #	Activity (e.g. Storage, Maintenance, Access to & Use of and Destruction Method)

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

Appendix 3: Video Surveillance Security Threat Assessment

To Determine the Requirements for a Video Surveillance System

Site Name: _____

Address: _____

Name of Requestor: _____ Division: _____

Date: _____ Video #: _____

Proposed Video Location: _____

- 1) Is there already a video surveillance system and/or camera on site? If yes, please describe and advise if its set-up adheres to the Chatham-Kent Video Surveillance Policy? (Use separate page if required)

- 2) Video surveillance should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable. Have the following security counter-measures been considered and rejected as unworkable?

#2	Security Counter-Measure	Yes	No	Comments
a.	Security Procedures			
b.	Duress Buttons			
c.	Door Locking Hardware			
d.	Alarm System			
e.	Access Control System			
f.	Signage			
g.	Security Guard/Officer Patrols			
h.	Lighting			
i.	Noisemaker devices			
j.	Other: Crime Prevention Through Environmental Design Audit (CPTED), etc)			

- 3) The use of each video surveillance camera should be justified on the basis of 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 Formats	Yes	No	Comments
a.	Corporate Security Occurrence Reports			
b.	Police Reports			
c.	Internal Memos			
d.	Other:			

Policy: Video Surveillance Policy	Section: 1 –	Issued:
--	---------------------	----------------

- 4) Consultation should be conducted to consider any systemic issues that may determine whether or not a video surveillance system will disparately impact disadvantaged group in the Municipality. Have the following equity considerations been reviewed?

#4	Equity Considerations	Yes	No	Comments
a.	Is the proposed camera being installed in a neighbourhood with historically excluded or marginalized groups?			
b.	Could the use of video surveillance disproportionately impact historically excluded or marginalized communities?			
c.	Have relevant community groups or municipal departments/divisions been consulted to mitigate any potential impacts of video surveillance on historically excluded or marginalized communities?			

- 5) An assessment should be conducted on the effects that the proposed video surveillance system may have on personal privacy and the ways in which any adverse effects can be mitigated. Have the following effects and mitigation strategies been considered?

#5	Effects & Mitigation Strategies	Yes	No	Comments
d.	The location of the proposed camera is situated in an area that will minimize privacy intrusion?			
e.	Is the proposed camera location one where the public and employees do not have a higher expectation of privacy (i.e., not in a washroom or change room, etc)?			
f.	Is the location of the proposed video camera visible?			
g.	Can the video surveillance be restricted to the recognized problem area?			
h.	Is space allocated for proper video surveillance signage?			
i.	Has a drawing been attached showing the video location?			
j.	Other:			

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

#6	Measures to Mitigate Effects	Yes	No	Comments
a.	Can the proposed camera be restricted through hardware or software to ensure that Operators cannot adjust or manipulate cameras to overlook spaces that a threat assessment has not been completed for?			
b.	Is the reception equipment going to be located in a strictly controlled access area?			
c.	Can the Video Surveillance Monitor be installed in such as way that it will be hidden from public view?			

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

d.	Can the Video Surveillance system be configured to only operate at times or periods of higher risk for the recognized problem area?			
e.	Other:			

Comments:

Completed by (Print Name and Position): _____

Signature: _____

Date: _____

DRAFT

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

Appendix 4: Video Surveillance Policy Training Checklist

Employee or Service Provider's Name:
Municipal Division or Company:
Position Title:

General Statement

The Information and Privacy Commissioner of Ontario published “Guidelines for Video Surveillance Cameras in Public Places” that forms the basis of the Municipality’s Video Surveillance Policy. These guidelines state 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 these “...training programs addressing staff obligations under the Act should be conducted on a regular basis”.

The Municipality intends to meet these obligations through the use of this Training Checklist and formal training completed on a regular basis in consultation with the Facility Video Supervisor and each Director.

1) **Policies and Procedures**

#	Question	Yes	No	Comments
a.	Has received a copy of, read and understood the Chatham-Kent Video Surveillance Policy?			
b.	Has received a copy of, read and understood the applicable appendices to the Chatham-Kent Video Surveillance Policy?			
c.	Has read and understood Chatham-Kent’s Corporate Policies and Forms, including but not limited to, Employee Code of Conduct Policy, IT Acceptable Use Policy, Web Portal Governance Policy, Request Form regarding Freedom of Information and Protection of Privacy, and Record Retention By-Law?			

2) **Roles and Responsibilities**

#	Question	Yes	No	Comments
a.	Understands the roles and responsibilities of the Municipal Clerk as FOI Coordinator, Directors, Facility Video Supervisors, Operators, municipal Employees, and Service Providers?			
b.	Understands and will carry out the duties and responsibilities of the Operator?			

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

3) Guidelines for the Implementation of a Video Surveillance System

#	Question	Yes	No	Comments
a.	Is aware that video surveillance equipment should only be installed and used to monitor those spaces that have been identified as requiring video surveillance?			
b.	Is aware that no person shall adjust or manipulate cameras to overlook spaces that are not intended to be covered by the video surveillance program?			
c.	Is 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, change rooms, etc.)			
d.	Is aware that all video surveillance installations must be clearly marked to advise staff and members of the public that video surveillance is in use?			
e.	Is aware that signs shall be posted at all entrances and/or on the perimeter of the grounds under video surveillance?			

4) Video Surveillance Equipment / Records

#	Question	Yes	No	Comments
a.	Has read, understood, and will follow the requirements for Record Identification, as stated in the Chatham-Kent Video Surveillance Policy?			
b.	Is aware that each Video Surveillance Operator shall maintain a logbook to record all activities related to video surveillance devices and records and that each entry will detail authorized staff, date, time, and activity?			
c.	Is aware that Operators 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?			
d.	Is aware that Operators may 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 any logbook?			
e.	Is aware that Operators shall not make any changes to the identification or labels of records either in hardcopy or computerized formats?			
f.	Is aware all storage devices that are not in use must be securely stored in a locked receptacle located in an access-controlled area?			
g.	Is aware that Operators shall not make any copies of data/images in any format (ex. hardcopy, electronic, etc.) from the video surveillance system without approval from the Facility Video Supervisor or Director, following the protocols in the Video Surveillance Policy?			

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

5) Access to Video Surveillance Records

#	Question	Yes	No	Comments
a.	Is aware that Operators may access information only when necessary to perform work assigned by a Facility Video Supervisor to accomplish the Municipality's mission and objectives?			
b.	Is aware that Operators must not access or use information from any component(s) of the Video Surveillance system files or database for personal reasons?			
c.	Is aware that access to the video surveillance records (i.e., logbook entries, CD's, videotapes, etc.) shall be restricted to authorized personnel only?			
d.	Is aware that the Operator shall not disclose personal information and that disclosure should only occur by the Facility Video Supervisor in consultation, as necessary, with the Director, to ensure that information is being disclosed in accordance with the <i>Municipal Freedom of Information & Protection of Privacy Act and Personal Health Information Protection Act</i> ?			
e.	Is aware of and understands the Formal Access Request process and the use of the "Access / Correction Form"?			

6) Viewing Images

#	Question	Yes	No	Comments
a.	Understands that video surveillance monitors should be concealed as much as possible from the general public and unauthorized employees?			
b.	Understands when recorded images from the camera must be viewed (i.e., for law enforcement or investigative reasons) this must occur in a private, controlled area that is not accessible to other staff and/or visitors?			

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

7) Retention and Disposal of Records

#	Question	Yes	No	Comments
a.	Is aware that an Operator must not dispose, destroy, or erase any record without proper authorization and without following the regulations contained in the Video Surveillance Policy?			
b.	Is aware that with the exception of requests by Law Enforcement agencies for copies of video surveillance recordings specific to a reported incident / investigation, Chatham-Kent does not maintain a copy of recordings provided in response to a law enforcement request?			
c.	Understands that video surveillance records will only be retained for a 60 day period depending upon the type of technology for non-incident recording?			
d.	Understands that the Operator shall take all reasonable efforts to ensure the security of records in the Municipality's custody and control?			
e.	Understands that all storage devices must be disposed of in accordance with an applicable technology asset disposal process ensuring personal information is erased, shredded, or burned and cannot be retrieved or reconstructed?			

8) Unauthorized Access and/or Disclosure

#	Question	Yes	No	Comments
a.	Understands that any Operator and/or any Chatham-Kent staff member who becomes aware of any unauthorized disclosure of a video surveillance record in contravention of the Chatham-Kent Video Surveillance Policy and/or a potential privacy breach are to immediately notify the Facility Video Supervisor or the Director?			
b.	Understands that a breach of this policy by an employee may result in discipline up to and including dismissal. A breach of this policy by service providers (contractors) to Chatham-Kent may result in termination of their contract?			

Policy: <i>Video Surveillance Policy</i>	Section: 1 –	Issued:
---	---------------------	----------------

9) Inquiries from the Public

#	Question	Yes	No	Comments
a.	Is aware that any Operator receiving an inquiry from the public regarding the Video Surveillance Policy shall direct the inquiry to their Director?			

10) Audit

#	Question	Yes	No	Comments
a.	Is aware that the Facility Video Supervisor will designate staff to conduct random audits to ensure the Video Surveillance Policy is being followed?			

Completed by (Print Name and Position): _____

Signature: _____

Date: _____

Witnessed by (Facility Video Supervisor name and Position): _____

Witness Signature: _____

Date: _____