POLICY No. 2014-03

Security Video Surveillance Systems

Originating Department	CMS-FP-01-2014		
SMT Approval:	2014-03-27		
Council in Committee:	2014-04-22	**Recommendation #:**	16
Council Approval:	2014-04-28	**Resolution #:**	67-14
Revision History:	Click here for revision history		

1. PURPOSE

This Policy has been developed to govern security video surveillance at County-owned/operated/leased facilities in accordance with the privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act (*MFIPPA*) "the Act".

Video surveillance, when used with other security measures, is an effective means of ensuring the security and safety of County facilities, the individuals who use them and the assets housed within them. The need to ensure security and safety however, must be balanced with an individual's right to privacy. The purpose of this Policy is to establish guidelines which are intended to achieve this balance. Specifically, this Policy addresses requirements and responsibilities with respect to:

- the installation of video surveillance systems;
- the operation of video surveillance systems;
- the use of the information obtained through video surveillance systems; and
- custody, control and access to records created through video surveillance systems.

2. POLICY

Application:

This Policy applies to all types of camera surveillance systems, surveillance monitors and camera recording devices that are used for security purposes at County-owned/operated/leased facilities. This policy does not apply to video surveillance used for employment-related or labour-related information. This policy does not apply to the videotaping or the audiotaping of County Council meetings.

Scope:

This Policy applies to all County facilities and to all County employees, Library Board employees and service providers.

Use of Information Collected:

The information collected through video surveillance is used only:

- to investigate an incident involving the safety or security of people, facilities, or assets;
- to provide law enforcement agencies with evidence related to an incident under police investigation;
- to provide evidence as required to protect the County's legal rights;
- to respond to a request for information under the Municipal Freedom of Information and Protection of Privacy Act;
- to investigate an incident involving an insurance claim that involves Haldimand County.

Public Consultation:

Haldimand County acknowledges the importance of public consultation when new or additional video surveillance systems for County facilities are being considered. The extent of public consultation may vary depending on the extent of public access. When new or additional video surveillance installations are being considered for County buildings to which the public has access – for example, the administration building, satellite offices, libraries, museums and arenas – consultation would not be required. When new or additional video surveillance installations are being considered for open public spaces such as streets or parks, the County shall consult with relevant stakeholders to determine the necessity and the acceptability of the proposed installation.

Notification to the Public:

Notification requirements under Section 29(2) of *MFIPPA* include informing 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 of personal information. The public shall be notified, using clearly written signs displayed at the entrance to and perimeter of, video surveillance areas so that the public has reasonable warning that surveillance is or may be in operation. Signs shall be of consistent size, format and wording.

A notice will also be posted on the Freedom of Information page on the County website.

Factors to Consider Prior to Using Video Surveillance Systems:

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

- The use of video surveillance cameras should be justified on the basis of specific reports of incidents, crime or significant safety concerns.

- A video surveillance system should be considered only after other measures of deterrence have been considered and rejected as unworkable.
- The proposed design and operation of the video surveillance system should minimize privacy intrusion.

Installation of Video Surveillance Systems:

Video surveillance equipment will only be installed in identified public areas where surveillance is deemed necessary to ensure the ongoing safety of County facilities, the individuals who use them and the assets that are housed in them.

Video equipment will be installed to monitor only the areas requiring video surveillance and will not be directed to look onto adjacent property.

Video surveillance equipment should never monitor the inside of areas where the public and employees have an expectation of privacy, such as change rooms or washrooms. Individual use of video or still photo devices, including video/digital cell phones, is also prohibited in these areas.

Video surveillance equipment may operate up to twenty-four (24) hours a day, seven (7) days a week within the system's capabilities.

Video monitors (reception equipment) will be located in controlled access areas. Where a separate, locked area cannot be provided, access will be restricted by password.

Operation of Video Surveillance Systems:

Division Managers are authorized to designate staff to operate video surveillance systems. The Manager will maintain a list of all persons designated and only those who have been designated may be permitted to operate the system.

The Manager or designate is responsible for establishing an appropriate training program for the operation of the equipment, including operator responsibilities with respect to protection of privacy and confidentiality.

Access to Information Collected:

Access to the video surveillance records (including logbooks) shall be restricted to authorized personnel only in order to comply with their roles and responsibilities as outlined in this Policy.

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

Personal Information Requests:

An individual whose personal information has been collected by a video surveillance system has a right of access to his or her personal information under Section 36 of the Act.

All personal information requests shall be made in writing and directed to the Freedom of Information (FOI) Coordinator on the prescribed form. The FOI Coordinator will provide direction to staff to provide this information or part thereof in accordance with the Act.

Access to personal information may depend on whether there is an unjustified invasion of another individual's privacy and whether any exempt information can reasonably be severed from the record.

The FOI Coordinator may charge fees for this service in accordance with *MFIPPA*.

Public Requests for Access to Information:

In accordance with the Act, any person may make a written request to the FOI Coordinator for access to digital records obtained by or through the use of the surveillance system by completing the County's Application for Access or Correction to Records form and by submitting the non-refundable, mandatory application fee.

The FOI Coordinator will review the legal authority of such person to receive the requested information, as indicated by *MFIPPA*.

The FOI Coordinator may charge additional fees for this service according to *MFIPPA* or in accordance with Haldimand County's Fee By-law where applicable.

When access to a record is given, the following information will be included in the FOI Coordinator's access logbook for audit purposes:

- the date and time of the original incident;
- the date and time at which the access was allowed or the date on which disclosure was made;
- the reason for allowing access or disclosure;
- the extent of the information for which access was allowed or which was disclosed; and
- provisions for the return of the record or its destruction.

Requests for Access to Video Surveillance Records by a Law Enforcement Agency:

If access to a video surveillance record is required for the purpose of a law enforcement investigation, the requesting officer must complete the "Law Enforcement Officer Request" form and forward it to the FOI Coordinator.

The FOI Coordinator will review requests on a case-by-case basis to determine whether disclosure will be granted. Depending on the nature of the request, law enforcement agencies may be required to complete a formal Freedom of Information request.

If the FOI Coordinator permits disclosure, a completed "Record of Release to Law Enforcement Agency" form will be copied to the IS Division Manager for record production.

A copy of the disclosed information will be provided to the FOI Coordinator for filing with the original release form. A copy of the release form will be provided to the law enforcement agency at the time of disclosure.

When a video recording is viewed or removed for law enforcement purposes, the access logbook entry shall include:

- the date and time of the original recorded incident;
- the date and time the record was provided to the requesting officer;
- the name and contact information of the requesting officer;
- whether the record will be returned or destroyed after use by the law enforcement agency.

Privacy Breach:

A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are not in accordance with the provisions of the Act.

When faced with a potential breach of privacy, the first two priorities are *containment* and *notification*.

Any County employee having knowledge of a privacy breach must immediately inform the divisional Manager of the breach. The Manager will inform the FOI Coordinator and together they will take all reasonable actions to recover the record and limit the record's exposure (containment). The FOI Coordinator will notify those individuals whose privacy was breached and advise of the steps that have been taken to address the breach, both immediate and long-term, including contacting the Information and Privacy Commissioner of Ontario (notification).

The FOI Coordinator will conduct an internal investigation to review the circumstances surrounding the breach and work together with the Information and Privacy Commissioner to make any necessary changes to policies and procedures.

Training:

Where applicable and appropriate, the Policy will be incorporated into training and orientation programs.

Retention Period of Information:

The retention period for information that has not been viewed for law enforcement or public safety purposes shall be fourteen (14) days. Recorded information that has not been viewed will be routinely erased.

Information that has been viewed by County staff, but does not appear to present any information pertinent to the protection of corporate assets or the safety of the public and employees, will be automatically erased through the re-write process.

When recorded information has been viewed for law enforcement or public safety purposes, the materials will be retained for a period of one (1) year from the date of the resolution of the incident.

The FOI Coordinator will retain logs in a secure manner for one (1) year.

The County shall store and retain retrieved records required for evidentiary purposes according to standard procedures until the law enforcement officers request them.

Retrieved and stored information will be disposed of securely and in such a manner that the personal information cannot be reconstructed or retrieved (physically destroyed, burned, magnetically erased or copied over).

Audits and Evaluations:

The Managers of the County divisions responsible for each County-owned or operated site with a video surveillance system shall conduct an annual audit to ensure that video surveillance continues to be justified in accordance with the requirements listed under "Factors to Consider Prior to Using Video Surveillance Systems."

The FOI Coordinator will ensure that any formal or informal information requests from the public have been tracked, and that reported incidents and police contact are properly recorded in the logbook.

Employees and service providers should be informed that their activities are subject to audit.

Review of Policy:

This policy shall be reviewed every two (2) years by the Manager of Facilities and Parks Operations (FAPO), in consultation with the FOI Coordinator and Manager of Community Development and Partnerships. The Manager of Facilities and Parks Operations will include recommendations for update, if any, in a report to Council.

3. DEFINITIONS

In this Policy:

3.1. "Facility" means any building or land that is either owned, occupied or leased by the County, including but not limited to, administration buildings, arenas, libraries, community halls, swimming pools, parks and cemeteries.

3.2. "Disclosure" means the release of relevant information which includes, but it is not limited to, viewing a recording, as well as making a copy of a recording.

3.3. "Privacy Breach" is the retention, collection, use or disclosure of personal information in ways that are not in accordance with the provisions of the Act.

The definitions below are taken from the Information and Privacy Commissioner/Ontario's "Guidelines for Using Video Security Surveillance Cameras in Public Places."

3.4. "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 an individual's race, colour, national or ethnic origin, sex and age. 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" under the Act.

3.5. "Record" is defined in Section 2 of MFIPPA as any record of information, however recorded, whether in printed form, on film, by electronic means or otherwise and includes: a photograph, a film, a microfilm, a videotape, a machine-readable record and any record that is capable of being produced from a machine-readable record.

3.6. "Video Surveillance System" refers to 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 personal information about individuals in open, public spaces (including streets, highways, parks). The term "video surveillance system" includes an audio device, thermal imaging technology or any other component associated with capturing the image of an individual.

3.7. "Reception Equipment" refers to the equipment or device used to receive or record the personal information collected through a video surveillance system, including a camera or video monitor or any other video, audio, physical or other mechanical, electronic or digital device.

3.8. "Storage Device" refers to a videotape, computer disk or drive, CD ROM, computer chip or other device used to store the recorded data or visual, audio or other images captured by a video surveillance system.

4. RESPONSIBILITIES

4.1. The Manager of Facilities & Parks Operations (FAPO) is responsible for the overall Corporate Video Surveillance Program and the management of authorized video security systems, including assisting other Managers with specifications, equipment standards and installation. The FAPO Manager will report to Council when a new video surveillance system is proposed.

4.2. The Manager of Information Systems or designated staff, is responsible for assisting with evaluation of video surveillance equipment to be procured and installation and operation of equipment, making a copy of a record in approved circumstances and overseeing the disposal of any storage device.

4.3. The FOI Coordinator will respond to requests for access to video surveillance records from the public and law enforcement agencies, respond to appeals and privacy complaints through the Office of the Information and Privacy Commissioner of Ontario, notify the Information and Privacy Commissioner of Ontario in the event of a privacy breach where appropriate and charge fees for the production of records in accordance with MFIPPA. The FOI Coordinator will also document 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 create a proper audit trail.

4.4. Division Managers responsible for each County-owned/operated/leased site with a video surveillance system are responsible for the life-cycle management of authorized video security surveillance systems and signage, including: recommending proposed installations in their divisions after assessing and documenting, in writing, any security threats; preparing a floor plan identifying the location of all video surveillance equipment at the site; implementing any site-specific procedures that may be required, including conducting periodic internal audits to ensure compliance with the Policy; ensuring that appropriate staff are familiar with the Policy and providing training; maintaining a record of personnel who are authorized to access and operate the system; posting a "Notice of Collection of Personal Information"; assigning a person or persons to be responsible for the day-to-day operation of the system in accordance with this Policy and conferring with the Manager of Information Systems for appropriate disposal of video surveillance systems.

4.5. County staff entrusted to operate or monitor the video surveillance system for a particular facility will:

- comply with all aspects of the Video Surveillance Policy;
- sign a Haldimand County Employee Undertaking of Confidentiality Form;
- monitor the video surveillance cameras as necessary;
- ensure no personal information is disclosed without the approval of the FOI Coordinator;
- ensure that no copies of data/images in any format are taken from the video surveillance system without approval from the FOI Coordinator.

4.6. All employees must adhere to the Policy and must not access or use information contained in the video surveillance system, its components, files or database for personal reasons, nor dispose, destroy or alter any record without proper authorization. All employees must also report any suspected privacy breach to their Manager.

4.7. County employees who knowingly or deliberately breach the policy or the provisions of the Act may be subject to disciplinary action up to and including, but not limited to, termination of employment.

4.8. Service providers, consultants and contractors shall review and comply with the Policy and MFIPPA in performing their duties related to the operation of the video surveillance system. The County will require all applicable service providers to the video surveillance system, consultants or other contractors who require access to the system to sign an agreement regarding their duties under this Policy and the Act, including a "Service Provider Undertaking of Confidentiality" form.

4.9. Where a service provider, consultant or other contractor fails to comply with this Policy or the provisions of the Act, it will be considered a breach of contract and may lead to penalties up to and including, but not limited to, contract termination.

5. ATTACHMENTS & REFERENCES

5.1. Site Specifics

5.1.1. Schedule A – Haldimand County Public Library, Caledonia and Dunnville Branches

5.1.2. Schedule B – Haldimand County Facilities and Parks

5.1.3. Schedule C – Grandview Lodge

5.1.4. Schedule D – Haldimand County Environmental Services

5.2. Municipal Freedom of Information and Protection of Privacy Act

5.3. Guidelines for Using Video Surveillance Cameras in Public Places (Information Privacy Commissioner document)

5.4. Public Libraries Act

REVISION HISTORY					
REPORT	CIC		COUNCIL		DETAILS
	Date	Rec#	Date	Res#	
	Date	Rec#	Date	Res#	
	Date	Rec#	Date	Res#	
	Date	Rec#	Date	Res#	
	Date	Rec#	Date	Res#	
	Date	Rec#	Date	Res#	

SCHEDULE A

Site Specifics – Haldimand County Public Library, Caledonia and Dunnville Branches

Security video surveillance systems are installed at two locations: the Dunnville Branch (7 cameras) and the Caledonia branch (9 cameras). Location maps are attached.

Background

The six branches of the Haldimand County Public Library have 165,000 visits per year. The Board and staff have put in place policies and staff training programs for promoting and maintaining a safe environment. In developing its policies and procedures, the Board is acting in accordance with the *Public Libraries Act*, which states that Library Boards may make rules for the use of library services, for the admission of the public to the library, for exclusion from the library of persons who behave in a disruptive manner or cause damage to library property.

Evidence has shown that all Haldimand County Library Branches experience some or all of the following:

- Theft of materials
- Unattended children
- Disruptive clients, including people with behaviour problems and problems with mental illness
- Criminal activity, including vandalism

As the two largest and busiest branches in the library system, Caledonia and Dunnville experience more safety issues and concerns because of the number of people using the branches, the longer opening hours and the difficulty of supervising a larger area. Video surveillance systems have been installed at these branches to enhance the safety of the public and employees and to detect and deter unlawful activities. Cameras are in areas that are unsupervised and/or beyond the normal sightlines of library staff.

Policies and Procedures

Library-specific:

- Patron Responsibility and Conduct Policy
- General Facility Use Policy
- Unattended Children in the Library Policy
- Internet Services Policy (including mandatory reporting of Internet Child Pornography)
- Emergency Manual

Haldimand County:

- Respect in the Workplace Policy
- Workplace Violence Policy
- Incident Reporting Procedures
- De-escalating Violence

Additionally, in accordance with the requirements of Bill 168, Library management staff conducted a workplace risk assessment and distributed a "Workplace Violence Survey" to employees.

Staff Training

- Dealing with Difficult People
- Workplace Violence Training
- Incident Reporting Procedures

Authorizations

All Library branch staff are authorized to perform live time viewing.

The following staff are authorized to review recorded information for a pre-defined occurrence:

- Library CEO
- Library Deputy CEO
- Library Branch Coordinator
- Other Library staff as required for purposes of identification
- Authorized security camera system contractor for maintenance purposes
- The IS Division Manager for the purposes of making a copy, where allowed under the provisions of *MFIPPA* and the Haldimand County Video Surveillance Policy
- The County FOI Coordinator for the purpose of processing requests for disclosure and appeals to the Information and Privacy Commission
- The Information and Privacy Commissioner during an appeal process
- Officers of law enforcement agencies, with the permission of the FOI Coordinator, for the purpose of obtaining evidence for investigation

The following staff are authorized to destroy information recorded on a hard drive:

- Manager, IS Division or designated staff

The following persons are authorized to destroy information on an alternate storage device:

- Manager, IS Division or designated staff
- Designates from a law enforcement agency who are in possession of copied images as required by their signed release form and in accordance with their retention schedules

SCHEDULE B

Site Specifics – Haldimand County Facilities and Parks

Security video surveillance systems are installed at five locations: the Caledonia Arena/HCCC (23 cameras); Caledonia Kinsmen Pool & Gazebo (11 cameras); Cayuga Arena (17 cameras); Dunnville Arena (21 cameras); Hagersville Arena (17 cameras). Location maps are attached.

Background

The Facilities and Parks Operations Division has installed cameras strategically at the above noted locations due to incidents of vandalism, criminal activity and disruptive clients. The size of these facilities makes certain locations vulnerable as supervisory staff cannot cover all of these areas concurrently.

Evidence has shown that all Haldimand County facilities experience some or all of the following:

- Vandalism
- Criminal activity
- Disruptive clients
- Unattended children

Policies and Procedures

- Respect in the Workplace Policy
- Workplace Violence Policy
- Public Conduct on Haldimand County Property
- Incident Reporting Procedures

Staff Training

- Dealing with Difficult People
- Workplace Violence Training
- De-escalating Violence

Authorizations

All Facilities and Parks Operations and Community Development and Partnerships staff are authorized to perform live time viewing.

The following Facilities and Parks Operations and Community Development and Partnership staff are authorized to review recorded information for a pre-defined occurrence:

- General Manager
- Manager
- Supervisor
-

- Administrative Assistant
- Lead Hand/Programmer
- Other staff as required for purposes of identification
- Authorized security camera system contractor for maintenance purposes
- The IS Division Manager for the purposes of making a copy, where allowed under the provisions of *MFIPPA* and the Haldimand County Security Video Surveillance Systems Policy
- The County FOI Coordinator for the purpose of processing requests for disclosure and appeals to the Information and Privacy Commission
- The Information and Privacy Commissioner during an appeal process
- Officers of law enforcement agencies, with the permission of the FOI Coordinator, for the purpose of obtaining evidence for investigation

The following staff is authorized to destroy information recorded on a hard drive:

- Manager, IS Division or designated staff

The following persons are authorized to destroy information on an alternate storage device:

- Manager, IS Division or designated staff
- Designates from a law enforcement agency who are in possession of copied images as required by their signed release form and in accordance with their retention schedules.

SCHEDULE C

Site Specifics – Grandview Lodge

A security video surveillance system is installed at Grandview Lodge: Grandview Lodge has a total of 9 cameras. Location maps are attached.

Background

Grandview Lodge has installed cameras strategically on the exterior and interior of the building because of the responsibility to care for 128 vulnerable residents, with possibility of criminal activity, vandalism and disruptive visitors. Grandview Lodge is a 24-hour a day operation which has staff coming into the building and leaving from 5:00 am until 11:30 pm. The centre core of the building is a vulnerable area during the late afternoon and early evening as these areas are not frequently attended by staff and the front doors are not locked until 9:00 pm to allow families to visit.

Evidence has shown that Grandview Lodge has experienced some or all of the following:

- Theft of materials
- Disruptive clients, including people with behaviour problems and problems with mental illness
- Criminal activity, including vandalism

Policies and Procedures

Grandview Lodge:

- Code White

Haldimand County:

- Respect in the Workplace Policy
- Workplace Violence Policy
- Incident Reporting Procedures
- De-escalating Violence

Additionally, in accordance with the requirements of Bill 168, Grandview Lodge staff conducted a workplace risk assessment and distributed a “Workplace Violence Survey” to employees.

Staff Training

- Dealing with Difficult People
- Workplace Violence Training
- Code White

Authorizations

All Grandview Lodge staff is authorized to perform live-time viewing.

The following staff is authorized to review recorded information for a pre-defined occurrence:

- General Manager of Community Services
- Grandview Lodge Administrator
- Grandview Lodge Supervisor of Facility Operations
- Grandview Lodge Director of Care
- Grandview Lodge Food Service Supervisor
- Grandview Lodge Programs Supervisor
- Other Grandview staff as required for purposes of identification
- Authorized security camera system contractor for maintenance purposes
- The IS Division Manager for the purposes of making a copy, where allowed under the provisions of MFIPPA and the Haldimand County Video Surveillance Policy
- The County FOI Coordinator for the purpose of processing requests for disclosure and appeals to the Information and Privacy Commission
- The Information and Privacy Commissioner during an appeal process
- Officers of law enforcement agencies, with the permission of the FOI Coordinator, for the purpose of obtaining evidence for investigation

The following staff is authorized to destroy information recorded on a hard drive:

- Manager, IS Division or designated staff

The following persons are authorized to destroy information on an alternate storage device:

- Manager, IS Division or designated staff
- Designates from a law enforcement agency who are in possession of copied images as required by their signed release form and in accordance with their retention schedules.

SCHEDULE D

Site Specifics – Haldimand County – Environmental Services

The Environmental Services Division currently has one security video surveillance camera installed at the Septage Receiving Station at the Dunnville Waste Water Treatment facility. Location maps are attached.

Background

The waste water treatment facilities within the County are contract-operated. The contracted operator is contractually responsible for the maintenance, repair and monitoring of the camera and facility referenced above.

The station itself is utilized by private contractors (waste haulers). As this facility may be accessed when the contracted operator may not be on-site there is a necessity to ensure that monitoring is provided to deter or detect incidents of theft and vandalism.

Policies and Procedures

A copy of this Policy will be provided to the contracted operator.

Haldimand County (for County staff that administer the contract):

- Respect in the Workplace Policy
- Workplace Violence Policy
- Incident Reporting Procedures

Staff Training (Haldimand County)

- Dealing with Difficult People
- Workplace Violence Training
- De-escalating Violence

Authorizations

The contracted Facility Operator – Project Manager, County Water & Wastewater compliance group team and Manager of Environmental Services are authorized to perform live time viewing.

The following contracted and County Environmental Services staff is authorized to review recorded information for a pre-defined occurrence:

Contracted Facility Operator:

- Project Manager
- Facility Operator
- Senior Operator

Haldimand County:

- General Manager Public Works
- Manager Environmental Services
- Water & Wastewater Compliance Supervisor
- Other Water & Wastewater staff as required for purposes of identification
- Authorized security camera system contractor for maintenance purposes
- The County FOI Coordinator for the purpose of processing requests for disclosure and appeals to the Information and Privacy Commission

External:

- The Information and Privacy Commissioner of Ontario during an appeal process
- Officers of law enforcement agencies, with the permission of the FOI Coordinator, for the purpose of obtaining evidence for investigation

The following staff is authorized to destroy information recorded on a hard drive:

- Manager, IS Division or designated staff

The following persons are authorized to destroy information on an alternate storage device:

- Manager, IS Division or designated staff
- Designates from a law enforcement agency who are in possession of copied images as required by their signed release form and in accordance with their retention schedules