Video Surveillance Policy

Section	Date	By-Law Number	Page	Of
Administration & Finance	~~April 20, 2018~~February 2026	29-2018	1	7
Subsection	**Repeals By-Law Number**		**Policy Number**	
Video Surveillance	80-2013		AF-1-3	

Policy Statement

The Corporation of the City of Kenora may use video surveillance on City properties and within City facilities only where such use is justified, necessary, proportionate, and connected to a lawfully authorized municipal purpose, including the safety of individuals, the security of municipal property, and the protection of City assets.

Video surveillance shall be implemented, operated, accessed, disclosed, retained, and disposed of in accordance with the Municipal Freedom of Information and Protection of Privacy Act, applicable records management requirements, and this Policy.

~~It is the policy of The Corporation of the City of Kenora to utilize video surveillance on City properties and within City facilities to ensure the safety of individuals and the security of City assets and property.~~

Commented [CF1]: The current statement is correct, but it should say more explicitly that surveillance is used only where justified, necessary, proportionate, and lawful. IPC guidance emphasizes that surveillance should not be adopted simply because it is convenient or useful; it should be tied to a lawfully authorized activity and used in a privacy-protective way.

Purpose

Video security surveillance systems are a resource used by The Corporation of the City of Kenora at selected City sites within the jurisdiction of the Corporation. In the event of a reported or observed incident, the review of recorded information may be used to assist in the investigation of the incident.

The City recognizes that video surveillance involves the collection of personal information and may affect individual privacy. Accordingly, this Policy establishes requirements for the lawful collection, use, disclosure, retention, security, and disposal of video surveillance records, as well as requirements respecting notice, privacy review, service provider management, access requests, and incident response.~~The City of Kenora recognizes that video surveillance technology has a high 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 the Municipal Freedom of Information and Protection of Privacy Act (the Act).~~

Commented [CF2]: Modern comparator policies and IPC guidance support a purpose statement that expressly covers collection, notice, access, disclosure, retention, safeguards, privacy review, and incident response. Cambridge uses wording like this. And wwe already have MFIPPA language in the Policy statement now.

This policy will provide guidelines designed to assist City Departments that have identified an appropriate use for video surveillance technology, to manage records that may be created using this technology in a manner that complies with the Act and records management requirements.

This policy also establishes minimum information technology (IT) controls to ensure the secure operation, storage, transmission, and lifecycle management of digital video surveillance systems.

Scope

These Guidelines do not apply to covert surveillance used for law enforcement purposes. In those circumstances, either a statutory authority exists and/or the authority for the surveillance is lawfully obtained through a search warrant.

Covert surveillance is conducted through the use of hidden devices. If covert surveillance is not implemented pursuant to the conditions in the preceding paragraph, extra diligence in considering the use of this technology is required. However, covert surveillance is beyond the scope of this policy.

This policy applies to all City-owned or City-managed video surveillance systems, including network-connected, IP-based, virtualized, or centrally managed systems, whether hosted on-premises or by an approved third-party service provider

Definitions

The Act **Act** means the *Municipal Freedom of Information and Protection of Privacy Act*, as amended.~~is with the privacy protection provisions of Ontario's Freedom of Information and Protection of Privacy Act (FIPPA) and Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).~~

Personal Information *has the meaning set out in the Act and includes recorded visual images of an identifiable individual captured by a video surveillance system.*~~*is* defined in Section 2(1) of FIPPA and 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, religion, 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*.~~

Commented [CF3]: Just simplifying

Consistent Purpose means a use of personal information that the individual to whom the information relates might reasonably have expected at the time of collection, within the meaning of the Act.~~is defined in Section 33 of MFIPPA as a use of personal information that the individual to whom the information relates might reasonably have expected at the time of collection.~~

Record means 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.

Video Surveillance System refers to any fixed, mobile, or network-connected electronic system or device that enables the collection, recording, viewing, or storage of visual images of identifiable individuals in public or City-controlled spaces.

~~***Video Surveillance System*** refers to a video, physical or other mechanical electronic or digital 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, sidewalks, highways, parks, trails and outside City facilities).~~

Reception Equipment refers to cameras, encoders, servers, network infrastructure, viewing stations, and administrative systems used to capture, transmit, process, or view video surveillance data

~~***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 that may be inside or outside City facilities.~~

Storage Device refers to any physical or electronic medium, including servers or secure digital storage systems, used to store recorded images.

~~***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.~~

~~Guidelines~~REQUIREMENTS

The following requirements apply to all City departments, employees, and service providers involved in the approval, operation, administration, maintenance, access, disclosure, retention, or disposal of video surveillance systems and records.~~The following guidelines are applicable to all City Departments.~~

Commented [CF4]: Calling the operative provisions "Guidelines" weakens the document. Much of what follows is mandatory policy content, not optional guidance.

1) Designated Responsibilities

The ~~City Clerk~~Manager of Information Technology is responsible for the overall Corporate Video Security Surveillance Program.

The Manager of each Department is responsible for ensuring the establishment of departmental procedures of video surveillance equipment, in accordance with this policy, and documenting the reason for implementation of a video surveillance system at a designated area.

The ~~Division Manager, as assigned by the Chief Administrative Officer,~~ Information Technology Manager is 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:

(a) Maintaining a record of the locations of the reception equipment, including noting the justification and purpose of the location.~~.~~
(b) Maintaining a list of personnel who are authorized to access and operate the system(s).
(c) Maintaining a record of the times when video surveillance will be in effect
(d) Posting of a NOTICE OF COLLECTION OF PERSONAL INFORMATION (Refer to Section 5).
(e) Assigning a person responsible for the day-to-day operation of the system in accordance with the policy, procedures and direction/guidance that may be issued from time-to-time.

The Information Technology Department is responsible for:

- establishing and maintaining technical security standards for video surveillance systems;
- managing network connectivity, authentication controls, and system access;
- supporting secure system maintenance, upgrades, and decommissioning.

~~(e)~~

(h) Employees and service providers with responsibilities under this Policy shall comply with the Act, this Policy, applicable procedures, and all confidentiality and security obligations.
(i) City employees may be subject to discipline where they knowingly or negligently breach this Policy, the Act, or related legal obligations.
(j) Any contract with a service provider that installs, hosts, supports, accesses, maintains, or stores video surveillance data shall require, at minimum:

1. recognition that records remain in the custody or control of the City for the purposes of the Act;
2. confidentiality and no secondary use of information;
3. access restrictions based on need-to-know;
4. prompt notification to the City of any actual or suspected privacy or security incident;
5. secure retention, return, and deletion requirements;

6. cooperation with City access requests, investigations, and audits; and
7. restrictions on subcontracting without City approval.

~~City employees and service providers shall review and comply with the policy and the Act in performing their duties and functions related to the operation of the video surveillance system.~~

~~City employees may be subject to discipline if they knowingly or deliberately breach the policy or the provisions of the Act or other relevant statutes.~~

~~Where the City has a contract with a service provider, the contract shall provide that failure by the service provider to comply with the policy or the provisions of the *Act* is considered a breach of contract leading to penalties up to and including contract termination. Employees of institutions and employees of service providers should sign written agreements regarding their duties under the policy and the *Act*, including an undertaking of confidentiality.~~

Commented [CF5]: Bill 194 and IPC guidance emphasizes privacy protections, and breach controls, and those are good best practices for municipal service-provider contracts as well. I just wanted clearer language.

2) Considerations

Prior to installation of video surveillance equipment, the City Department must consider the following:

(a) 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 or for crime prevention. Video cameras should only be installed in identified public areas where video surveillance is a necessary and viable detection or deterrence activity.

(b) A privacy review or privacy impact assessment must be completed before:

~~(c)~~ i. any new video surveillance installation;

~~(d)~~ ii. any material expansion of an existing system;

iii. any material repositioning or change in field of view;

iv. any material change in purpose, hours of operation, or functionality; or

v. any migration to a new hosting, storage, analytics, or managed service environment.

Formatted: Indent: First line: 0.5", No bullets or

Formatted: Indent: Left: 0.5"

Formatted: Indent: Left: 1"

Formatted: Indent: Left: 1", No bullets or numbering

Commented [CF6]: The current draft says an assessment "should" be conducted. That should become mandatory. IPC PIA guidance approach both support a structured privacy review before implementation or material change

~~(e) An assessment of the effects that the proposed video surveillance system may have on personal privacy should be conducted in an attempt to mitigate any adverse effects. Privacy intrusion should be minimized to that which is absolutely necessary to achieve its required, lawful goals.~~

~~(f)~~(c) A requirement that any agreements between the City and service providers state that the records dealt with or created while delivering a video surveillance program are under the City's control and subject to privacy legislation (MFIPPA).

~~(g)~~(d) A requirement that employees and service providers (in the written agreement) review and comply with the policy and the Act in performing their

duties and functions related to the operation of the video surveillance system.

3) Installation and Placement

(a) Video surveillance equipment should never monitor the inside of areas where the public and employees have a higher expectation of privacy such as change rooms and washrooms.

~~(b)~~ Monitoring stations, recording equipment, servers, administrative consoles, and other backend components of the video surveillance system shall be located in controlled-access environments and accessible only to authorized personnel. ~~Equipment should be installed in a strictly controlled access area. Only controlling personnel should have access to the access area and the equipment.~~

~~(c)~~ Video surveillance equipment shall be positioned and configured so that it captures only those areas necessary to achieve the approved purpose and avoids unnecessary collection from adjacent private property, private residences, workspaces, or other areas not relevant to the approved purpose, unless such collection is unavoidable and specifically documented. ~~Equipment should be installed in such a way that it only monitors those spaces that have been identified as requiring video surveillance.~~

~~(d)~~(b) Adjustment of the camera position should be restricted, if possible, to ensure only designated areas are being monitored.

~~(e)~~(c) Video surveillance should be restricted to periods when there is demonstrably a higher likelihood of crime being committed and detected in the area under surveillance, and may also be used to act as a deterrent to prevent further property loss.

(d) Signs should be clear, language-neutral graphical depiction of the use of video surveillance and prominently displayed at the perimeter of the monitored areas and at key locations within the areas. The signs should include basic information to clarify that video surveillance is being used in the area.

(e) Video surveillance systems shall be logically segmented from public networks and protected through firewalls or equivalent network security controls.

(f) Remote access to video systems shall be restricted, authenticated, logged, and enabled only where operationally required.

~~(f)~~(g)

Commented [CF7]: Just wanted to be more specific when it came to what equipment would be in controlled areas.

Commented [CF8]: This is an important part of the policy and should be strengthened. IPC guidance emphasizes limiting collection to what is necessary

4) Lawful Collection

Section 28(2) of MFIPPA establishes the conditions under which personal information may be collected. This section provide that no person shall collect personal information on behalf of an institution, unless the collection is:

a) expressly authorized by statute
b) used for the purposes of law enforcement or
c) necessary to the proper administration of a lawfully authorized activity

The Corporation of the City of Kenora "Municipality" is lawfully authorized to operate municipal facilities and in doing so, are required to take steps to ensure the safety of the individuals who visit such facilities.

Section 31(1) of MFIPPA restricts how personal information may be used once it has been lawfully collected. As a general rule, the act prohibits the use of personal information unless the municipality obtains consent from the individual to whom the information relates or the personal information is used for the purpose for which it was obtained or compiled or for a consistent purpose.

The City of Kenora collects video surveillance for the purpose of the video surveillance program only or for a consistent purpose.

5) Notification

The public should be notified of the existence of video surveillance equipment by clearly written signs prominently displayed at the entrances, exterior walls, interior of buildings and/or perimeter of the video surveillance areas.

Signage must satisfy the notification requirements under section 29(2) of the *Act,* which 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;

The following is suggested wording for use in building signage, based on a minimum requirement of the Information and Privacy Commissioner of Ontario:

"This area is monitored by video surveillance cameras. Please direct inquires to: *(title, business address and phone number of someone who can be contacted during business hours to answer questions about the collection of personal information)"*

6) Access, Use and Disclosure

Section 3 of Regulation 823 of MFIPPA requires the municipality to define, document and put in place reasonable measures to prevent unauthorized access as well as inadvertent destruction or damage of records. Information collected by way of video surveillance systems may only be used for the purposes of the stated rationale and objectives set out to protect public safety or to detect and deter criminal activity and vandalism. Information should not be retained or used for any other purposes.

(a) All video recordings, whether stored on physical media or digital storage systems (including on-premises, cloud-hosted, or Software-as-a-Service platforms), that are not actively in use shall be securely stored in a controlled access environment. Storage media shall be logically and/or physically protected, appropriately labeled where applicable, and safeguarded against unauthorized access, loss, or tampering.

~~(a) All tapes or other storage devices that are not in use should be dated, labeled and stored securely in a locked container located in a controlled access area.~~

(b) Access to video surveillance recordings and storage systems shall be restricted to authorized personnel only and protected through appropriate technical and administrative controls, including role-based access and authentication measures. All access to, and use of, recorded information shall be logged in a manner sufficient to create a reliable audit trail.

~~(b)~~(c) ~~Access to the storage devices should only be by authorized personnel. Logs should be kept of all instances of access to, and use of, recorded material to enable a proper audit trail.~~ The personal information recorded by video surveillance is subject to access and privacy legislation. An individual whose personal information has been collected by a video surveillance system has a right of access under Section 36 of the Municipal Freedom of Information and Protection of Privacy Act. Access will depend upon whether an exemption applies and if exempt information can be reasonably severed from the record.

c) Only the CAO, City Solicitor, General Manager, Division Manager or a delegated alternate, or law enforcement may review the information. Circumstances, which would warrant review, will normally be limited to an incident that has been reported/observed or to investigate a potential crime.

General access to City video surveillance for their own purpose is only permitted under general circumstances under section 4 of MFIPPA. Individuals may have access to their own personal information, however, another person's personal information may not be included unless consent is provided by that party. A Freedom of Information request must be filed with the Freedom of Information Officer to obtain this information and appropriate procedures and fees under that application followed.

Formatted: Font: Verdana, 11 pt

7) Lawful Disclosure

MFIPPA prohibits the disclosure of personal information, except in the circumstances identified in section 32 of MFIPPA. Personal information may be lawfully disclosed in limited circumstances to appropriate authorities for limited purposes.

All general requests for disclosure must be placed by filing a Freedom of Information request (FOI) through the Freedom of Information Officer with the City of Kenora.

Requests from enforcement agencies for the sole purpose of a police investigation may be filed directly with the City's IT department and appropriate logs for such requests will be retained. These logs will include the name of officer, enforcement agency requesting and the general nature of the investigation.

8) Retention

The retention period for information that has not been viewed for law enforcement, public safety purposes, or security of public property shall be thirty (30~~twenty one (21)~~ calendar days for digital systems. Once the retention period is met, all recordings are overridden by new video data.

When recorded information has been viewed for law enforcement or public safety purposes, the retention period shall be a minimum of one (1) year from the date of viewing. Unless involved in an active police investigation.

The City will store and retain storage devices required for evidentiary purposes according to standard procedures until the law enforcement authorities request them.

9) Training

Where applicable and appropriate, the policy and guidelines will be incorporated into training and orientation programs of the Corporation and service provider(s). Training programs addressing staff obligations under the Act shall be conducted as necessary.

Reference

The Municipal Freedom of Information and Protection of Privacy Act (MFIPPA); Information and Privacy Commissioner of Ontario (IPC) Guidelines for Using Video Security Surveillance Cameras in Public Spaces; The Municipal Act