SUBJECT: **VIDEO SURVEILLANCE POLICY**

Policy No: **2019-23**

Date: **December 2, 2019**

Next Review Date: **December 2023**

Number of Pages: **8**

PURPOSE

The purpose of this Video Surveillance Policy is to establish guidelines and procedures for using video surveillance cameras on any property and/or in any building owned or operated by the Innisfil Public Library Board as deemed necessary by the CEO.

POLICY

General

All Staff are committed to the goal of a safe Library. The video surveillance policy outlines one of the processes in place to ensure that library facilities are kept as safe as possible.

Application

Applies to all facilities operated by the Innisfil Public Library Board.

Definitions

Act refers to Ontario's *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56.*

Personal information is defined in Section 2 of Ontario's *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56* as being 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. Therefore, a simple image on a video surveillance system that is clear enough to identify a person, or the activities in which he or she is engaged, will be classified as "personal information" under the Act.

Record is defined in Section 2 of Ontario's *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56* to mean any information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a microfiche, 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 a video, physical or other mechanical, electronic or digital surveillance system or device that enables continuous or periodic video recording, observing or monitoring of individuals in open, public spaces. The Information and Privacy Commissioner of Ontario includes in the term video surveillance system, an audio device, thermal imaging technology, or any other component associated with recording the image of an individual.

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.

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

These guidelines were reviewed in conjunction with the *Guidelines for the Use of Video Surveillance* issued by the Information and Privacy Commissioner of Ontario in October 2015.

The video surveillance cameras will compliment other measures to ensure a safe and secure environment. The video cameras will be positioned to record only those identified areas.

The Innisfil Public Library Board under the Board's jurisdiction uses video surveillance equipment to promote the safety of customers, staff and the community. This equipment also helps to protect the Library's property against theft or vandalism and can assist in identifying intruders and persons breaking the law. 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 Library will maintain control of and responsibility for the video security surveillance system at all times. Employees and service providers are expected to review and comply with the policy, the Act, and other relevant statutes in performing any duties and functions that are related to the operation of the video security surveillance program. Employees who knowingly or deliberately breach the policy or the provisions of the Act or other relevant statutes may be subject to discipline. Service providers that knowingly or deliberately breach the policy or the provisions of the Act or other relevant statutes may be found to be in breach of the contract leading to penalties up to and including contract termination.

Responsibilities

The CEO, Deputy Chief Librarian, IT Manager, Area Managers or other designated employees at facilities are authorized to operate the systems. Library employees and service providers are to review and comply with the Policy, Guidelines, and relevant Acts in performing their duties and functions related to the operation of the video surveillance system.

CEO - The CEO or Deputy Chief Librarian is responsible for the overall Library video security surveillance program and is responsible for the Library's privacy obligations under Ontario's *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56* and this policy. The CEO or designate will coordinate audits.

IT Manager - The IT Manager and the IT Staff are responsible for the technical aspects of the equipment, its installation, maintenance and the retention and disposal of the recorded information.

The Library Board – The Library Board, through their designate, is responsible for the development and review of the policy and supporting guidelines and signage.

Area Managers – The Area Managers, in collaboration with the IT Manager as required, at a facility having a video surveillance system are responsible for the day-to-day operation of the system in accordance with the policy, guidelines, and direction/guidance that may be issued from time-to-time.

Collection of Personal Information Using a Video Surveillance System

Any recorded data or visual, audio or other images of an identifiable individual qualifies as "personal information" under the Act. The Library has determined that it has the authority to collect this personal information in accordance with the Act. Pursuant to section 28(2) of Ontario's *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56,* no person shall collect personal information on behalf of the Library unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity. The Library must be able to demonstrate that any proposed or existing collection of personal information by a video surveillance system is authorized under this provision under the Act.

Planning Considerations for Video Security Surveillance Systems

Before deciding if a facility warrants a video security surveillance system, the Library will consider the following:

1. A video security surveillance system should only be considered where less intrusive means of deterrence, such as increased monitoring by Staff and security guard patrols have been shown to be ineffective or unworkable.

2. Before implementing a video surveillance program, a facility should be able to demonstrate:
    a) A history of incidents occurring in the specific facility;
    b) The effect of the physical circumstances of the facility – does it permit ready access to unauthorized individuals; and
    c) Whether a video security surveillance program would be effective in dealing with or preventing future incidents of the type that have already occurred.

3. The acquisition, installation, and operation of individual video security surveillance systems should be justified on the basis of enhancing the safety of clients and Staff and/or deterring destructive acts such as vandalism.

4. An assessment should be conducted of the effects that the proposed video security surveillance system may have on personal privacy, and the ways in which any adverse effects can be mitigated.

5. Consultations should be conducted with relevant stakeholders as to the necessity of the proposed video security surveillance program at the facility.

6. The Library will endeavour to ensure that the proposed design and operation of the video security surveillance system minimizes privacy intrusion to that which is absolutely necessary to achieve its required lawful goals.

The Design, Installation and Operation of Video Security Surveillance Equipment
In designing, installing and operating a video security surveillance system, the Library will consider the following:

1. Reception equipment such as video cameras, or audio or other devices should be installed in identified public areas where video surveillance is a necessary and viable detection or deterrence activity. The equipment will operate up to 24 hours/seven days a week, within the limitations of system capabilities (e.g. digital), power disruptions and serviceability/maintenance.

2. The equipment should be installed in such a way that it only monitors those spaces that have been identified as requiring video surveillance. Cameras should not be directed to look through the windows of adjacent buildings.

3. If cameras are adjustable by operators, this should be restricted, if possible, so that operators cannot adjust or manipulate them to overlook spaces that are not intended to be covered by the video surveillance program.

4. Equipment should never monitor the inside of areas where the clients, staff and the public have a higher expectation of privacy (e.g. change rooms and washrooms).

5. Clearly written signs, prominently displayed at the entrances, exterior walls, and/or the interior of buildings which have video security surveillance systems, shall provide Staff and the public with reasonable and adequate warning that video surveillance is in effect. Signage will satisfy the notification requirements under section 29(2) of Ontario's *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56, 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.

   As a minimum, there should be a sign in place that notifies individuals of the recording and informs them that they may contact Library Administration offices with any questions. The remainder of the notice requirements under the Act can be satisfied through information pamphlets available in the facility and on our web site. The CEO, Deputy Chief Librarian and the Area Managers will be the 'Point-of-Contact' for the Library's branches.

6. The Library will endeavour to be as open as possible about the video security surveillance program in operation and upon request, will make available to the public, information on the rationale for the video surveillance program, its objectives and the policies and guidelines that have been put in place. This may be done in a pamphlet or on our web site.

7. Reception equipment should be in a strictly controlled area. Only personnel authorized in writing by the CEO, Deputy Chief Librarian or the IT Manager should have access to the controlled access area and the recording equipment. Video monitors should not be in a position that enables public viewing.

8. The maintenance program for reception and recording equipment will include optimizing and lens cleaning while ensuring that the equipment is operating properly and in accordance with the manufacturer's specifications. Library Staff will endeavour to promptly follow-up on issues or concerns regarding the performance of the equipment.

Access, Use, Disclosure, Retention, Security and Disposal of Video Security Surveillance Records

Any information obtained through the video security surveillance systems may only be used for the purposes set out in the policy and must relate to the protection of clients, staff and the public, including the discipline or consequences that arise from that, or it must assist in the detection and deterrence of criminal activity and vandalism.

Information should not be retained or used for any purposes other than those described in the policy. Video security surveillance should not be used for monitoring staff performance. Since video security surveillance systems create a record by recording personal information, each facility having a system will implement the following procedures:

1. Storage devices should be stored securely in a locked receptacle located in a controlled-access area. Logs should be kept of all instances of access to, and use of, recorded material to enable a proper audit trail.

2. Procedures on the use and retention of recorded information include:
   a) Only the CEO, Deputy Chief Librarian, IT Manager, Area Manager and delegated alternates (designated by name and position) 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. Real-time viewing of monitors may be delegated by the CEO, and/or IT Manager, to a limited number of individuals.
   b) Video may be disclosed to the police when:
      - The law enforcement agency approaches your institution with a warrant requiring the disclosure of the footage, as per section 42 (1) (e) of FIPPA, and section 32 (e) of MFIPPA;
      - The law enforcement agency approaches your institution without a warrant, and asks that you disclose the footage to aid an investigation from which a proceeding is likely to result, as per section 42 (1) (g) of FIPPA, and section 32 (g) of MFIPPA; or
      - You observe an illegal activity on your premises and disclose the footage to a law enforcement agency to aid an investigation from which a proceeding is likely to result, as per section 42 (1) (g) of FIPPA and section 32 (g) of MFIPPA.
   c) The retention period for information that has not been viewed for law enforcement, library or public safety purposes shall be a minimum of five (5) days but not to exceed 28 calendar days (four weeks) for digital systems. These time-frames are based on risk assessment, privacy considerations, and equipment capabilities. Recorded information that has not been used in this fashion, within these time-frames, is then routinely erased in a manner in which it cannot be reconstructed or retrieved.
   d) When recorded information has been viewed for law enforcement, branch, or public safety purposes, the retention period shall be one year from the date of viewing. Section 5 of Ontario Regulation 823 under Ontario's *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56,* requires that personal information that has been used must be retained for one year.

3. The Library will store and retain storage devices required for evidentiary purposes according to standard procedures until the law enforcement authorities request them. A release form will be completed before any storage device is disclosed to appropriate authorities. The form will indicate who took the device, under what authorities, when this occurred, and if it will be returned or destroyed after use. This activity will be subject to audit.

4. Old storage devices must be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved. Disposal methods could include shredding, burning or magnetically erasing the personal information. A record of the disposal is to be completed and retained.

5. Any customer, Staff Member or member of the public who has been recorded by a video security surveillance camera has a general right of access to his or her personal information under section 36 of Ontario's *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56*. This right is recognized. One exemption that may apply is contained in subsection 38(b) of Ontario's *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56*, which grants the heads of an institution the discretionary power to refuse access where disclosure would constitute an unjustified invasion of another individual's privacy. As such, access to an individual's own personal information in these circumstances may depend upon whether any exempt information can be reasonably severed from the record. One way in which this may be achieved is through digitally "blacking out" the images, where technically possible, of other individuals whose images appear on the recording(s).

6. The application of the frivolous or vexatious request provisions of Ontario's *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56,* would occur in very rare circumstances. It can be concluded that a request for access to a record or personal information is frivolous or vexatious if:
   a) The opinion is, on reasonable grounds, that the request is part of a pattern of conduct that amounts to an abuse of the right of access or would interfere with the operations of the facility, or
   b) The opinion is, on reasonable grounds, that the request is made in bad faith or for a purpose other than to obtain access.

7. The CEO will respond to any inadvertent disclosures of personal information. Any breach of Ontario's *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56,* shall be reported to the CEO.

Training

Where applicable and appropriate, the policy and guidelines will be incorporated into training and orientation programs of the Library Staff. Training programs addressing staff obligations under the Act shall be conducted as necessary.

Auditing and Evaluating the Use of a Video Surveillance System

The Library will ensure that the use and security of video security surveillance equipment is subject to regular audits. The audit will address the Library's operational compliance with the policy and the guidelines. An external body may be retained in order to perform the audit. The Library will endeavour to address any deficiencies or concerns identified by the audit as soon as possible. Employees and service providers should be aware that their activities are subject to audit and that they may be called upon to justify their surveillance interest in any given individual. The Library will regularly review and evaluate its video surveillance program to ascertain whether it is still justified in accordance with the planning requirements set out in this document.

This evaluation shall occur at least once every three years and will include the review/update of the policy and the guidelines.

Related Policies
Facility Security Policy

Approved by the Innisfil Public Library Board, December 2, 2019
Motion Number: 2019.82

Supersedes Policy #2014-11, approved April 22, 2014, Motion #2014.29; &
#2011-09, approved April 18, 2011, Motion #2011.27; &
Policy #2008-08, approved April 21, 2008, Motion #2008.25; &
Policy #2005-05, approved June 13, 2005, Motion #2005.33.