**BIBLIOTHÈQUE PUBLIQUE DU CANTON DE RUSSELL**
**TOWNSHIP OF RUSSELL PUBLIC LIBRARY**

| | |
|---|---|
| **Type of policy :** | Operational Policy |
| **Title of policy :** | Security Video Surveillance Policy |
| **Policy number :** | **3.5.4** |
| **Date of approval :** | |
| **Dates of modifications :** | |
| **Date of next review :** | **2020** |

## STATEMENT OF PURPOSE

The purpose of the Security Video Surveillance Policy is:
(1) to establish guidelines and procedures for using video surveillance cameras on any property and/or in any building operated by the Library;
(2) to ensure that, in adopting the use of video surveillance cameras, the Library recognizes and balances the security benefits with an individual's right to privacy;
(3) to ensure that the use of security cameras is in accordance with privacy legislation and the Library's Confidentiality and Privacy Policy.

## UNDERLYING PRINCIPLES

In the daily operation of Library premises, the safety of property, visitors, and employees is protected and maintained by conventional means such as: alert observation by staff, security-conscious design of Library locations, safe behaviour training, and the consistent application of basic rules of conduct. However, in some circumstances, the additional protection provided by surveillance cameras is essential to ensure the safety and security of clients and visitors and the lawful, safe and appropriate use of Library premises and property.

The guidelines of this Policy were developed in close consultation with the "Guidelines for Using Video Surveillance Cameras in Public Places" issued by the Information and Privacy Commissioner of Ontario (2007 revised edition).

## POLICY STATEMENT

The Library recognizes the need to balance an individual's right to privacy and the need to ensure the safety and security of Library employees, clients, visitors and property. While video surveillance cameras are installed for safety and security reasons, the Library's video surveillance systems are designed and maintained to minimize privacy intrusion.

## GUIDELINES

### A. DEFINITIONS

***MFIPPA*** refers to the Ontario Municipal Freedom of Information and Protection of Privacy Act.

***Personal information*** is defined in section 2 of the Ontario Municipal Freedom of Information and Protection of Privacy Act 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.

***Record*** is defined in section 2 of the Ontario Municipal Freedom of Information and Protection of Privacy Act 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.

***Incident Report*** means a report prepared by staff or security personnel that details an incident involving the public on Library property.

***Video Surveillance Device or 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.

***Camera*** refers to a device that converts images into electrical signals for television transmission, video recording, or digital storage.

***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 any other device used to store the recorded data or visual, audio or other images captured by a video surveillance system.

## B. REGULATIONS

### 1. Planning considerations, design and installation guidelines

(a) Planning Considerations

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

- the use of video surveillance cameras is justified to address significant safety or security issues;
- other measures of deterrence or detection have been considered and rejected as ineffective or unworkable;
- an assessment has been conducted on the effects that the proposed video surveillance may have on personal privacy, and the ways in which any adverse effects can be mitigated;
- the proposed design and operation of the video surveillance systems minimizes privacy intrusion.

(b) Design and Installation Guidelines
When designing a video surveillance system and installing equipment, the following must be considered:
- video surveillance systems may operate up to 24 hours/seven days a week, within the limitations of system capabilities (e.g. digital), power disruptions and serviceability/maintenance;
- video equipment shall be installed to monitor only those spaces that have been identified as requiring video surveillance;
- video surveillance cameras shall be limited to areas where the public and library staff have no reasonable expectation of privacy;
- every reasonable attempt will be made by authorized personnel to ensure video monitors are not in a position that enables the public to view the monitors.

**2. Notice of use of video systems**
The public shall be notified through appropriate signage that surveillance is or may be in operation before entering a surveillance area. Signage will satisfy the notification requirements under section 29(2) of the MFIPPA which includes 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 name, title and contact information of the staff member responsible for answering questions about the surveillance.

**3. Personnel Authorized to Operate Video Equipment**
Only authorized personnel shall be permitted to operate video surveillance systems.

**4. Video Desktop Monitors**
- Only authorized personnel shall be permitted to view video desktop monitors and have access to real-time images.
- Since video cameras may not be continuously monitored, the public and staff should take appropriate precautions for their safety and for the security of their personal property.

**5. Video Recordings**
(a) Use of Records
The records collected through video surveillance are used:
•To monitor or investigate any incident involving the safety or security of patrons, staff, volunteers and/or contractors;
•To monitor or investigate any incident involving the safety or security of any library branch;
•To monitor or investigate an incident related to the conduct of patrons, staff, volunteers or contractors;
•To investigate an incident involving violations of the Library's Workplace Violence Prevention Policy and Workplace Harassment Policy;
•To provide evidence as required to protect the Library's legal rights;
•To provide law enforcement agencies with evidence related to an incident under police investigation.
Video recordings will not be used for the purpose of routine staff performance

evaluations.

(b) Retention Period
- Video surveillance recordings will be retained for a minimum period of seven (7) working days and a maximum period of twenty-eight (28) working days. These time-frames are based on risk assessment, privacy considerations and equipment capabilities. As new images are recorded, the oldest images will be automatically erased and deleted.
- Archiving of records beyond twenty-eight (28) days, where there are reasonable grounds that the date may be required for a specific investigation and/or follow-up must be approved by the Chief Executive Officer or his/her designate.
- Records required for evidence shall be saved to a secure file and stored in a secure environment. Such records will be destroyed after two (2) years unless they are still required for evidence and/or pursuant to any applicable legislation.
- In cases where a patron has been banned by the Library, the record(s) will be retained for a period of up to six (6) years, or for the period of the ban, whichever is longer.

(c) Access
- Access to video surveillance recordings shall be restricted to authorized personnel, and only in order to comply with their roles and responsibilities as outlined in this Policy.
- All formal requests to access video surveillance recordings should be directed to the Chief Executive Officer or his/her designate.
- If the Library receives a request from the general public to access security camera recordings, the requester will be advised to file a police complaint.
- Access to a record may be provided to a third party (e.g. an individual whose image has been recorded and retained) – in that instance, a formal request must be made in writing to the Chief Executive Officer or his/her designate. The processing of a request will be subject to the requirements of privacy legislation and pursuant to Regulation 823 of MFIPPA.
- If access to a video surveillance recording is required for the purpose of a law enforcement investigation, the requesting Officer must complete a Disclosure of Personal Information Form and forward it to the Chief Executive Officer, or his/her designate. The Chief Executive Officer will provide the recording for the specified date and time of the incident requested by the Law Enforcement Officer, subject to MFIPPA exemptions.
- For audit purposes, logs will be kept of all instances of access to, and use of, records. The log will include the name, date, time and reason for the viewing access.

(d) Viewing Recordings
When recorded images from the cameras must be viewed for law enforcement or investigative reasons, this must only be undertaken by authorized personnel, in a private, controlled area that is not accessible to other staff and/or visitors.

(e) Custody, Control, Retention and Disposal of Video Records/Recordings
- The Library retains custody and control of all video recordings. Video recordings are subject to the access and privacy requirements of MFIPPA, which include but are not limited to the prohibition of all Library employees from access or use of information from

the video surveillance system, its components, files, or database for personal reasons.
- The Library will take all reasonable efforts to ensure the security of records in its control/custody and their safe and secure disposal.

(f) Unauthorized Access and/or Disclosure (Privacy Breach)
- Any Library employee who becomes aware of any unauthorized disclosure of a video record in contravention of this Policy, and/or a potential privacy breach has a responsibility to ensure that the Chief Executive Officer or his/her designate is immediately informed of the breach.
- Once a privacy breach has occurred (loss, theft, or inadvertent disclosure of personal information) immediate action will be taken to control the situation. The Chief Executive Officer or his/her designate will:
(i) identify the scope of the breach and take steps to contain the damage (e.g., determine if unauthorized access to the system has occurred, retrieve copies of recorded information, etc.);
(ii) inform the Information and Privacy Commission and, if applicable, notify affected parties whose personal information was disclosed;
(iii) conduct an internal investigation into the matter to review the circumstances surrounding the event as well as the adequacy of existing policies and procedures in protecting personal information;
- A breach of this Policy by Library staff may result in disciplinary action up to and including dismissal.
- A breach of this Policy by service providers (contractors) to the Library, may result in termination of their contract.

**6. Inquiries from the Public**
- All inquiries regarding the Video Security Surveillance Policy shall be directed to the Chief Executive Officer or his/her designate.

**7. Audit and Evaluation**
A regular evaluation and audit of the library's video surveillance systems will be performed to ensure its compliance with legislation and Library policies and procedures.

**8. Accountability**
a. **The Chief Executive Officer** is responsible for:
- implementing this Policy;
- approving the installation of video surveillance systems after a safety or security assessment has been completed;
- reporting to the Board when video surveillance is proposed for a location;
- maintaining the log of all instances of access to, and use of, video surveillance records;
- documenting, implementing, enforcing, monitoring and updating the Library's privacy and confidentiality compliance;
- undertaking regular evaluation of the library's video surveillance systems to ensure compliance with this Policy;
- ensuring Library Branch Heads are familiar with this Policy;
- ensuring training in compliance with this Policy is available and provided to appropriate staff and service providers;

- responding to formal requests to access records, including law enforcement inquiries;
- investigating privacy complaints related to video surveillance records, and security/privacy breaches.

b. **Library Branch Heads** are responsible for:
- overseeing the day-to-day operation of video surveillance cameras, providing supervision to approved authorized personnel, and ensuring their compliance with all aspects of this Policy;
- ensuring library staff under their supervision are familiar with this Policy;
- ensuring monitoring and recording devices, and all items related to the surveillance systems are stored in a safe and secure location;
- immediately reporting breaches of security/privacy to the Chief Executive Officer or his/her designate.

## REFERENCES

Guidelines for the use of video surveillance cameras in public spaces - 2007 (Information and Privacy Commissioner of Ontario)

Township of Russell Public Library Confidentiality and Privacy Policy (Policy 3.3.9.1)

Municipal Freedom of Information and Protection of Privacy Act, R.R.O. 1990, c. M. 56 (MFIPPA)

Municipal Freedom of Information and Protection of Privacy Act, R.R.O. 1991, Regulation 372/91 as amended