POLICY: **Security Camera Policy**		POLICY NO: **OP 10**
CATEGORY: **Operational**	LAST REVIEW / REVISION DATE: February 2024	SCHEDULED REVIEW DATE: February 2027

Security Camera Policy

Stratford Public Library strives to maintain a safe and secure environment for visitors and staff. In pursuit of this objective, selected public areas of the library premises are under security camera coverage. This Security Camera Policy aims to ensure that the Library balances the security benefits derived from the use of security cameras with the privacy rights of the individual.

Use of security cameras at library facilities is part of the organization's overall strategy to ensure the safety of persons and property. This Policy ensures that the Library follows the guidelines set out by the Information and Privacy Commission/Ontario, and the privacy requirements of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) without compromising the safety and security of library visitors, staff and premises.

This Policy applies to all types of camera surveillance systems, surveillance monitors and camera recording devices that are used for security purposes at the Stratford Public Library. This Policy does not address instances where staff record a specific event (such as a program, or presentation).

Collection of Personal Information

Any recorded data of an identifiable individual qualifies as "personal information" under MFIPPA. Security cameras can be used to collect personal information about identifiable individuals. Stratford Public Library has determined that it has the authority to collect this personal information in accordance with the MFIPPA. Pursuant to section 28(2) of the Ontario MFIPPA, no person will collect personal information on behalf of the organization unless the collection is expressly authorized, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

Design, Installation and Operation of Security Cameras

When designing a security camera system and installing equipment, the following must be considered:

1. Given the open and public nature of the library facility and the need to provide for the safety and security of employees and visitors who may be present at all hours of the day, the security camera coverage systems may operate at any time in a 24-hour period.
2. The ability of authorized personnel to adjust cameras will be restricted so that authorized personnel cannot adjust or manipulate cameras to overlook spaces that are not intended to be covered by the security camera coverage program.
3. Equipment will never monitor the inside of areas where the public and employees have a higher expectation of privacy (e.g. washrooms).
4. Recording equipment must be located in a strictly controlled access area. Only authorized personnel will have access to the controlled access area and the recording equipment.
5. Regular maintenance of recording equipment will ensure that the equipment is operating properly. Staff will endeavor to promptly follow-up with issues or concerns regarding the performance of equipment.

Signage

The library will post signs visible to members of the public at all entrances and other designated areas indicating security cameras are in use.

Use of Records

1. Staff may be authorized to monitor real-time camera feeds as is reasonably necessary to implement this Policy. Every reasonable attempt will be made to ensure security camera monitors are not in a position that enables the public to view them.
2. Only the Chief Executive Officer, Technology and Operations Manager, library supervisors or other authorized delegates may review recorded information from the system.
3. Security camera footage will not be used to monitor employee performance. Circumstances which warrant review, will be limited to security incidents for example: vandalism, theft, break-in or violation of the Library's Code of Conduct.
4. All storage devices will be located in a controlled-access area. Access to the storage devices will be limited to authorized personnel. Logs will be kept of all instances of access to, and use of, recorded material to enable a proper audit trail.
5. The Library will take all reasonable efforts to ensure the security of records in its control/custody and ensure their safe and secure disposal.
6. Security camera systems will be set-up to ensure regular recordings are cleared or overwritten on a regular basis. Normally, systems will be set-up to maintain records for up to 14-21 days. In some cases, system capacity may limit the time records are maintained. In cases where the security camera system records activities that relate to an insurance, liability, law enforcement or other similar issue, the appropriate section of the recording will be copied to suitable media and stored in a separate secure location for a period of no less than one (1) year or a longer appropriate length of time.

Logs

The library must maintain a log that records all activities related to security cameras and records. Activities include all information regarding the use, maintenance, and storage of records and all instances of access to, and use of, recorded material, including the name of the person accessing the system. All logbook entries will detail staff name, date, time, date and time of incident, requestor and note regarding the request for footage.

Access Request Process

All requests to view security camera coverage will be directed to the Chief Executive Officer or designate.

Law Enforcement Access Request

If access to security camera coverage is required for the purpose of a law enforcement investigation, the law enforcement officer must provide a badge number or investigation number in order to obtain the data from the CEO or designate. The CEO or designate will provide the recording for the specified date and time of the incident requested by the law enforcement officer, subject to MFIPPA exemptions.

When records are released to law enforcement officials, where possible, authorized staff will limit the release of information about individuals deemed not to be involved in the investigation. This includes, but is not limited to, zooming images in on suspects in question, obscuring identifiable features of other individuals and limiting the time frame of video coverage provided.

Viewing Images

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

Training
Staff with responsibilities under this Policy will be made aware of their obligations under MFIPPA, and training will be conducted accordingly.

Breach of Policy
A 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 CEO is immediately informed of the breach.

The following actions will be taken immediately:

- Library staff will take all reasonable actions to recover the record and limit the record's disclosure.
- Affected parties whose personal information was inappropriately disclosed will be notified.
- If applicable and upon confirmation of the existence of a privacy breach, the CEO or designate will notify the Information and Privacy Commission of Ontario (IPC) and work constructively with the IPC staff to mitigate the extent of the privacy breach, and to review the adequacy of privacy protection with the existing Policy.
- Senior staff will investigate the cause of the disclosure with the goal of eliminating potential future occurrences.

A breach of this Policy may result in disciplinary action up to and including dismissal. A breach by service providers or contractors to the Library may result in termination of the contract.

Related Documents
- OP 04 Customer Code of Conduct
- Municipal Freedom of Information and Protection of Privacy Act
- Ontario Human Rights Code
- Canadian Charter of Rights and Freedoms
- Guidelines for the Use of Video Surveillance Cameras (Information and Privacy Commissioner, 2015)

ORIGINAL DATE ADOPTED	February 13, 2024	Review Cycle	Every 3 years
REVIEW/APPROVAL HISTORY			