Policy Name:	**Security Video Surveillance**
Policy Type:	**Operational**
Policy Number:	**OP-14**
Original Adoption Date:	**June 2012**
Current Approval:	**September 2025**
Review:	**November 2028**
Motion:	**2025:66**

Security Video Surveillance

1. **Purpose:**

The Security Video Surveillance Policy provides direction concerning the context and protocols within which the Library installs and operates surveillance cameras to help maintain a safe space for staff and the public. The Policy ensures that the Library follows the guidelines set out by the ***Information and Privacy Commissioner of 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.

2. **Policy:**

The Orillia Public Library strives to maintain a safe and secure environment for members of the public and staff. In pursuit of this objective, selected public areas of the Library premises are under video surveillance. This Policy aims to ensure that, in adopting the use of security video surveillance cameras, the Library balances the security benefits derived from the use of video surveillance with the privacy rights of the individual.

3. **Procedure**

Section 1 – Design, Installation and Operation of Security Cameras

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

Policy Name:	**Security Video Surveillance**
Policy Type:	**Operational**
Policy Number:	**OP-14**
Original Adoption Date:	**June 2012**
Current Approval:	**September 2025**
Review:	**November 2028**
Motion:	**2025:66**

i. The Library's security camera coverage systems may operate at any time in a 24-hour period, given the open and public nature of the Library's facilities and the need to provide for the safety and security of employees and visitors who may be present at all hours of the day.

ii. Only authorized personnel may adjust the cameras. Camera positioning must prevent coverage of areas not intended for surveillance.

iii. Equipment shall never monitor the inside of areas where the public and employees have a higher expectation of privacy (e.g. washrooms).

iv. Live view/recording equipment must be located in a strictly controlled access area. All staff may have access to real-time controlled areas to ensure public and staff safety. However, only authorized personnel shall have controlled access to the recording and play-back equipment.

v. Authorized personnel must receive training prior to becoming authorized, to understand the technical and policy requirements.

Section 2 – Notice of Use of Video Systems

a. In order to provide notice to individuals that video is in use:

i. The Library shall post signs, visible to members of the public, at all entrances and/or prominently displayed on the perimeter of the grounds under security camera coverage. On at least one sign at each location with security camera coverage the following information will include:

- The legal authority for the collection of personal information.
- The principal purpose(s) for which the personal information is intended to be used.

ii. Additional signs will be used to support awareness of the security camera program.

iii. The Security Video Surveillance Policy will be posted on the Library's website.

Section 3 – Security Camera Monitors and Records

a. Security camera footage is not actively used to monitor members' use of Library spaces or employee performance. Circumstances which warrant review will be limited to security incidents that have been reported, investigation of a potential crime, or identifying individuals associated or potentially involved with a crime. Footage may also be used to assist in identifying or resolving property-related matters. Access will be limited to cases where review of camera footage may help to identify the cause of/or help resolve a problem.

b. All storage devices will be located in a controlled-access area. Logs will be kept of all instances of access to, and use of, recorded material to enable a proper audit trail. 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 and activity.

c. The Library will take all reasonable efforts to ensure the security of records in its control/custody and ensure their safe and secure disposal.

d. Security camera systems will be set-up to ensure regular recordings are cleared or overwritten on a regular basis. Systems will be set-up to maintain records for up to 14 days. If authorized staff need to remove information from the system (still images, video footage) for authorized reasons, the resulting record(s) will be securely maintained for at least one (1) year.

Policy Name:	**Security Video Surveillance**
Policy Type:	**Operational**
Policy Number:	**OP-14**
Original Adoption Date:	**June 2012**
Current Approval:	**September 2025**
Review:	**November 2028**
Motion:	**2025:66**

Section 4 – Access Requests

a. All approved requests to view security camera coverage will be recorded in the Log and will be directed to the CEO or designate. Requests will be reviewed based on Library policy and relevant legislation including ***MFIPPA***.
b. If a member of the public wishes to see video following an alleged crime, they must report it to the Police and Police may request access to the footage or go through a Freedom of Information Request which is subject to ***MFIPPA***.
c. If access to a security camera coverage record is required for the purpose of a law enforcement investigation, the requesting Officer must complete the Disclosure of Personal Information Form and forward it to the CEO or designate (see OP-14 Appendix A). 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.
d. When recorded images from the cameras must be viewed for law enforcement or authorized staff for investigative reasons, this must only be undertaken by authorized personnel, in a private, controlled area that is not accessible to other staff and/or members of the public.

Section 5 – Unauthorized Access and/or Disclosure (Privacy Breach)

a. Any Library employee who becomes aware of an 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.
b. The following actions will be taken immediately in accordance with OPL's procedures for managing a privacy breach:

i. Upon confirmation of the existence of a privacy breach, the CEO or designate will notify the ***Information and Privacy Commissioner of Ontario (IPC).***

ii. Staff will 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.

iii. The CEO or designate in consultation with the Director of the department in which the breach of Policy occurred, shall investigate the cause of the disclosure with the goal of eliminating potential future occurrences.

iv. The staff member will work with the Director and the CEO or designate to take all reasonable actions to recover the record and limit the record's disclosure.

v. The CEO, where required, shall notify affected parties whose personal information was inappropriately disclosed.

vi. A breach of this Policy 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.

Related Documents:

- ***Information and Privacy Commissioner of Ontario***
- ***Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), 1990***
- Orillia Public Library: Addressing Violence in the Workplace (HR-08)
- Orillia Public Library: Code of Conduct (OP-03)
- Orillia Public Library: Employee Code of Conduct (HR-10)

- Orillia Public Library: Privacy, Access to Information and Electronic Messages (OP-01)
- OP-14 Appendix A: Disclosure of Personal Information