

Policy: Security Video Surveillance

Board motion number: 28:21, April 13, 2021 Chairperson's signature: _____

Policy Objective

The Bonnechere Union Public Library Board of Trustees has determined the need for the acquisition and installation of a surveillance camera system. This decision was based upon past incidents and a perceived level of risk for safety of staff, patrons and service providers.

The purpose of the Video Surveillance Policy is to describe the Library's installation and use of video surveillance equipment in the interests of privacy, public safety, protection of property, and to maintain a safe and welcoming environment for library patrons, staff, and service providers. Video surveillance deployment is guided by the principle of minimal intrusion into the daily operation of library facilities, patron confidentiality and staff privacy.

Underlying Principles

Underlying the Policy Objective is Bonnechere Union Public Library's commitment to maintaining a safe and welcoming environment for staff and members of the public. Bonnechere Union Public Library (BUPL) will achieve this through a modern, cohesive security system that strives to minimize intrusions upon the personal privacy of patrons, staff, and service providers. Video surveillance will only be reviewed for the purpose of investigation of incident or complaint, or for a formal request received by the Information and Privacy Commissioner of Ontario in accordance with the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

The Security Video Surveillance Policy provides detailed direction concerning the context, procedures, and protocols within which the Library installs and operates surveillance cameras. 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. The guidelines mentioned above will be made available to patrons who request it for the sake of transparency.

Designing and Installing Video Surveillance Equipment

When designing the video surveillance system and installing the equipment, the following were considered:

1. Given the open and public nature of the Library's facilities and property, and the need to provide for the safety and security of individuals who may be present at all hours of the day, the Library's video surveillance systems may operate at any time in a 24-hour period. The audio capabilities will not be enabled;
2. The video equipment shall be installed to monitor only those spaces that have been identified as requiring video surveillance;
3. The ability of authorized personnel to adjust cameras shall be restricted to the CEO or Acting Manager;
4. Equipment shall never monitor the inside of areas where the public and employees have a higher expectation of privacy (e.g. washrooms, staff room and makerspace);
5. Reception/recording equipment must be located in a strictly controlled access area. Only authorized personnel shall have access to the controlled access area and the reception/recording equipment. Remote viewing will be disabled;
6. Monitors are not used for BUPL's surveillance system at this time. Use of them would require approval from the Board.

Notice of Use of Video Systems

In order to provide notice to individuals that video is in use, the Library shall display signs, visible to members of the public, at all entrances and/or on the perimeter of the area under video surveillance;

The notification requirements of this sign must inform individuals of:

- the legal authority for the collection of personal information;
- the principle 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.

Personnel Authorized to Operate Video Equipment

Only authorized personnel shall be permitted to operate video surveillance systems. Authorized personnel refers to the CEO or Acting Manager.

Video Equipment/Records

Types of Recording Device

The Library may use either recording mechanisms that record information directly on a hard-drive or recording mechanisms using a removable/portable storage device in its video systems. Records are to be retained in accordance with the retention periods specified in this Policy.

Records will be retained on the video system hard drive for a 30-day period and periodically backed up. Then, retained for a full year after which they will be expunged.

Record Identification

All records shall be clearly identified (labeled) as to the date and location of origin including being labeled with a unique, sequential number or other verifiable symbol.

Record Keeping

The CEO will handle all disclosure requests that are received either electronically or in paper format, and will notify the Board when a request is received. The CEO and Board members must discuss and approve all requests before action is taken. The staff, board members and the CEO are not to retain copies of images of a request on their personal devices. The form will be stored with other confidential material in the Library.

Access to Video Records

Access

Access to the video surveillance records shall be restricted to authorized personnel, and only in order to comply with their roles and responsibilities as outlined in the Security Video Surveillance Policy.

Storage

All storage devices that are not in use must be stored securely in an access-controlled area, for example the safe.

Formal Access Requests Process

All formal requests for video records should be directed to the CEO. Requests are subject to the requirements of MFIPPA and the Library's Access to Information and Protection of Privacy Policy.

Access: Law Enforcement

If access to a video surveillance record is required for the purpose of a law enforcement investigation, the requesting Law Enforcement Officer must complete the Disclosure of Personal Information Form and forward it to the CEO. The CEO will notify the Board and will provide the recording for the specified date and time of the incident requested by the Law Enforcement Officer, subject to MFIPPA exemptions.

It is important to complete the Disclosure of Personal Information Form when requesting video surveillance footage. The Disclosure of Personal Information Form serves as the record for the request and is maintained and stored by the CEO with the Library's confidential files.

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.

Custody, Control, Retention and Disposal of Video Records/Recordings

The Library retains custody and control of all original video records not provided to law enforcement. Video records are subject to the access and privacy requirements of MFIPPA, which include but are not limited to the prohibition of all Library employees and Library Board from access or use of information from the video surveillance system, its components, files, or database for personal reasons.

The CEO will make all reasonable efforts to ensure the security of records in the Library's control/custody and ensure their safe and secure disposal. Old storage devices (ones exceeding the retention period) or defective storage devices must be disposed of in accordance with an applicable technology asset disposal process ensuring personal information is erased prior to disposal, and cannot be retrieved or reconstructed. Disposal methods may include shredding, burning, or erasing depending on the type of storage device.

Records and information collected from the video recording system are subject to the following retention periods:

Information will be retained for a maximum of one year from the date of the original collection by the video surveillance system, except when information collected from the video recording system will be used by the Library or a law enforcement agency as part of a criminal, safety, or security investigation or for evidentiary purposes. In which case, information will be retained for a minimum of one (1) year from the conclusion of the matter for which it has been used.

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 CEO and the Chair of the Board are immediately informed of the breach. The entire Board must then be advised of the situation by the Chair.

Inquiries from the Public Related to the Video Surveillance Policy

A staff member receiving an inquiry from the public regarding the Video Surveillance Policy shall direct the inquiry to the CEO.

Accountability

The Board is responsible for:

- Approving the installation of video surveillance cameras, and for Investigating privacy complaints related to video surveillance records, and security/privacy breaches.
- Complying and adhering to all aspects of this policy.

The CEO is responsible for:

- Documenting, implementing, and enforcing the Library's privacy and access compliance policies;
- Ensuring that all aspects of the video recording system are functioning properly;
- Ensuring features that are available yet prohibited are not enabled. i.e.: audio recording, remote viewing;
- Responding to formal requests to access records, including law enforcement inquiries;
- Ensuring that no video surveillance imagery/records are disclosed without the approval of the Board;
- Ensuring that access to video surveillance occurs within the guidelines in this Policy (documentation of a potential criminal act may also result in the access of video surveillance);
- Providing advice, training, and recommendations to staff to assist in compliance with MFIPPA;
- Undertaking periodic evaluation of the video surveillance system to ensure compliance with this Policy;
- Reviewing this Policy on a regular basis, and recommending updates as appropriate to the Board;
- Ensuring training in compliance with this Policy is available and provided to appropriate staff and service providers; and
- Investigating privacy complaints related to video surveillance records, and security/privacy breaches. Board should be part of investigations.

Staff are responsible for:

- Complying with and adhering to all aspects of this Policy;
- Forwarding all requests for access to video records to the CEO;
- Immediately reporting breaches of security/privacy to the CEO or designate; and
- Forwarding all inquiries from the public about the use of video surveillance or about the Library's Security Video Surveillance Policy to the CEO.

Appendices

Appendix 1: References

Guidelines for Using Video Surveillance, Information and Privacy Commissioner of Ontario. 2015.

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.

Occupational Health and Safety Act, R.S.O. 1990, c.0.1.

Bonnechere Union Public Library Safety, Security and Emergency Policy.

Appendix 2: Definitions

Authorized staff: Employees of BUPL or of a BUPL contractor who are specifically authorized by the Library to operate the video surveillance system and to perform the duty, responsibility or action described in the Policy.

Video surveillance operation: Operation of the video surveillance system may include:

1. Requesting access to video surveillance records
2. Accessing/viewing/retrieving video surveillance records
3. Disposing of video surveillance records
4. Installing/maintaining video surveillance systems and infrastructure