



Video Surveillance

Operational

Policy

Statement

The Brantford Public Library (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, customers, and property. While video surveillance cameras are installed for safety and security reasons, the Library's video surveillance systems must also be designed to minimize privacy intrusion.

Proper video surveillance, where deemed necessary, is one of the most effective means of helping to keep the Library facilities and property operating in a safe, secure, and privacy protective manner.

Description

This Library policy has been developed to govern video surveillance at existing and future Library Branches in accordance with the privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

Application

This policy applies to all types of camera surveillance systems, surveillance monitors and camera recording devices at Library Branches that are used for security purposes.

Responsibilities

The CEO/Chief Librarian is responsible for the Video Surveillance Policy.

Roles and Responsibilities

Responsibilities of CEO/Chief Librarian

The CEO/Chief Librarian may delegate various responsibilities under this Policy to managers. The CEO/Chief Librarian:

- Is responsible and accountable for documenting, implementing, enforcing, monitoring and updating the Library's privacy and access compliance;

- Will report to the Board when video surveillance is being proposed for locations and will prepare annual reports to the Board on all new security video surveillance systems installed;
- Informs appropriate shared facilities' personnel of this Policy's requirements if in a shared facility.

Managers

Managers are responsible for:

- Recommending proposed installations in their department after reviewing security threat assessments;
- Ensuring that appropriate library staff are familiar with this Policy and providing advice, training and recommendations to staff to assist in compliance with MFIPPA;
- 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 monitoring and recording devices, and all items related to surveillance (e.g. logbooks) are stored in a safe and secure location;
- Ensuring logbooks recording all activities related to security video devices and records are kept and maintained accurately by authorized personnel;
- Responding to formal requests to access records, including law enforcement inquiries, in consultation with the CEO/Chief Librarian or designate;
- Investigating privacy complaints related to video surveillance records, and security/privacy breaches;
- Immediately reporting breaches of security/privacy to the CEO/Chief Librarian or designate.
- Reviewing annually the video surveillance system and policy and recommending updates as appropriate to the CEO/Chief Librarian.

Responsibilities of Corporate Services Administrator

The Corporate Services Administrator, as designated by the CEO/Chief Librarian, is responsible for:

- Reviewing security threat assessments to determine requirements for a video surveillance system;
- Advising on installations and operation;
- Assessing proposed installations in accordance with this Policy in consultation with the appropriate manager;
- Conducting periodic internal audits to ensure compliance with this Policy;
- Delegating the day-to-day operations of video surveillance systems to managers and contracted security personnel and ensuring compliance with this Policy and BPL procedures;

The IT Department Staff

The IT Department staff are responsible for:

- Technical aspects of equipment, its installation and maintenance and the retention and disposal of the recorded information.

Contracted Security Personnel

Contracted security personnel, as designated by the CEO/Chief Librarian, shall be responsible for:

- Compliance with this Policy;
- Ensuring logbooks recording all activities related to security video devices and records are kept and maintained accurately by authorized personnel;
- Referring formal requests to access records, including law enforcement inquiries to management;
- Live monitoring of video surveillance systems;
- Ensuring computers systems are locked when unattended to prevent unauthorized access;
- At the direction of CEO/Chief Librarian, reviewing recordings to capture images and/or extract recordings for investigative purposes and/or to obtain evidence images for identifying individuals;
- Immediately reporting breaches of security/privacy to the CEO/Chief Librarian or designate.

Responsibilities of All Library Staff

All library staff must adhere to the Video Surveillance Policy and must not access or use information contained in the video surveillance system, its components, files, or database for personal reasons, nor dispose, destroy, erase or alter any record without proper authorization and without following the regulations contained in the Video Surveillance Policy.

Guidelines to Follow Prior to the Implementation of a Video Surveillance System

Factors to Consider Prior to Using Video

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

- The use of video surveillance cameras should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns.
- A video surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable.
- An assessment must be conducted on the effects that the proposed video surveillance system 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 should minimize privacy intrusion.

Designing and Installing Video Surveillance Equipment

When designing a video surveillance system and installing equipment, the following must be considered:

- Given the open and public nature of the Library's facilities and the need to provide for the safety and security of employees and customers 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 video equipment should be installed to only monitor those spaces that have been identified as requiring video surveillance.
- The ability to adjust cameras should be restricted, if possible, so that cameras cannot be adjusted or manipulated to overlook spaces that are not intended to be covered by the video surveillance program.
- Equipment should never monitor the inside of areas where the public and employees have a higher expectation of privacy (e.g. washrooms).
- Where possible, video surveillance should be restricted to periods when there is a demonstrably higher likelihood of crime being committed and detected in the area under surveillance.
- Reception/recording equipment must be located in a strictly controlled access area. Only designated staff, or those properly authorized in writing by the CEO/Chief Librarian or designate, shall have access to the controlled access area and the reception/recording equipment.
- Every reasonable attempt should be made to ensure video monitors are not in a position that enables the public and/or unauthorized staff to view the monitors.

Notice of Use of Video Systems

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

- 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 video surveillance;
- Signs must inform 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.

Personnel Authorized to Operate Video Equipment

Only employees designated by the CEO/Chief Librarian shall be permitted to operate video surveillance systems.

Video Records

The Library may use Digital Video Recorders (DVR). Facilities using video recorders will retain these records for a period of 30 days. A record of an incident will only be stored longer than the

30 days where it may be required as part of a criminal, safety, or security investigation or for evidentiary purposes.

Record Identification Logbook

All records (storage devices) shall be clearly identified (labelled) as to the date and location of origin including being labelled with a unique, sequential number or other verifiable symbol. In facilities with a DVR that stores information directly on a harddrive, the computer time and date stamp shall be understood to be this identification.

Electronic logbooks shall be maintained to record all activities related to video devices and records. The activities include all information regarding the use, maintenance, and storage of records and all instances of access to, and use of, recorded material. All logbook entries will detail authorized staff, date, time and activity. This logbook must be saved in a safe and secure file location.

Access to Video Records

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

Formal Access Requests Process

Any disclosure that is not in support of law enforcement will only be made in accordance with MFIPPA or as required by law. All requests for video records should be directed to the CEO/Chief Librarian or designate for processing. A person requesting access to a record should make a request in writing. The individual requesting the record must:

- Provide sufficient detail (the approximate time and date, the location - if known - of the incident, etc.) to enable an experienced employee of the Brantford Public Library, upon a reasonable effort, to identify the record; and,
- At the time of making the request, pay the prescribed fees as provided for under the Act.

Access: Law Enforcement

The Library will disclose video surveillances recordings to law enforcement agencies and/or security personnell to support law enforcement efforts. If access to a video surveillance record is required for the purpose of a law enforcement investigation, the requesting officer must complete the Library's Law Enforcement Disclosure form (see appendix #1) and forward this form to the CEO/Chief Librarian or designate. The CEO/Chief Librarian, or designate, will provide the recording for the specified date and time of the incident as requested by the law enforcement officer. The CEO/Chief Librarian, or designate, will record the following information in the facility's video logbook:

- i. the date and time of the original, recorded incident including the designated name/number of the applicable camera and DVR;
- ii. the name of the Operator at the time of the incident;
- iii. the time and date the copy of the original record was saved;
- iv. the time and date the saved record was provided to the requesting officer; and,

- v. if the record will be returned or destroyed after use by the law enforcement agency.

Viewing Images

When recorded images from the cameras must be viewed for law enforcement or investigative reasons, this must only be completed by an individual(s) authorized by the CEO/Chief Librarian in a private, controlled area that is not accessible to other staff and/or visitors.

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

The Brantford Public 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 the MFIPPA, which includes but is not limited to the prohibition of all Library staff from access or use of information from the video surveillance system, its components, files, or database for personal reasons. With the exception of records retained for criminal, safety, or security investigations or evidentiary purposes, the Library must not maintain a copy of recordings for longer than the recording systems' 30 day recording cycle.

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

Unauthorized Access and/or Disclosure (Privacy Breach)

Library staff who become aware of any unauthorized disclosure of a video record in contravention of this Policy and/or a potential privacy breach are to immediately notify the CEO/Chief Librarian. After this unauthorized disclosure or potential privacy breach is reported:

- Upon confirmation of the existence of a privacy breach, the CEO/Chief Librarian shall notify the Information and Privacy Officer 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.
- The CEO/Chief Librarian will work with the Corporate Services Administrator to take all reasonable actions to recover the record and limit the record's disclosure.
- The CEO/Chief Librarian, in consultation with the Corporate Services Administrator, and where required, will notify affected parties whose personal information was inappropriately disclosed.
- The CEO/Chief Librarian, in consultation with the Corporate Services Administrator shall investigate the cause of the disclosure with the goal of eliminating potential future occurrences. Intentional wrongful disclosure, or disclosure caused by negligence, by employees of the Library may result in disciplinary action up to and including dismissal. Intentional wrongful disclosure, or disclosure caused by negligence, by service providers (contractors) to the Library, may result in termination of their contract.

Inquires 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/Chief Librarian.

Review of Video Surveillance Policy

This policy shall be reviewed every 4 (four) years by the CEO/Chief Librarian who will forward recommendations for update, if any, to the Brantford Public Library Board for approval.

History

Supersedes: Not applicable

Background documents, related policies: Brantford Public Library Electronic Monitoring of Employees Policy; Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

Approval Date: December 2012

Revision History: April 2023

Projected Review Period: 2027

Author: Corporate Services Administrator

Approval Level: Brantford Public Library Board