

Purpose and Scope

Burlington Public Library strives to provide a safe and secure environment for customers, staff and property while protecting individual privacy rights.

Statement of Policy

The Library recognizes the use of security cameras at Library facilities as part of its overall strategy to ensure the safety of persons and property. This policy will adhere to privacy requirements set out in the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). In addition, this policy has been developed to follow the guidelines set out by the Information and Privacy Commission of Ontario.

Definitions

MFIPPA: Municipal Freedom of Information and Protection of Privacy Act. The purpose of the Act is to provide a right of access to information under the control of institutions and to protect the privacy of individuals with respect to personal information about themselves held by institutions.

IPC: Information and Privacy Commission of Ontario. IPC oversees compliance with the privacy protection provisions of MFIPPA and conducts investigations into privacy complaints. IPC also provides guidance regarding Ontario's access and privacy legislation.

Personal Information: identifiable information about an individual such as name, phone, address, email, date of birth, race, religion, colour, sex etc., and any correspondence between the individual and the organization which may or may not be confidential in nature. Exceptions and further definitions are defined in the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

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'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, the Library's security camera coverage systems may operate at any time in a 24-hour period.
2. The ability of authorized personnel to adjust cameras shall 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 shall never monitor the inside of areas where the public and employees have a higher expectation of privacy (e.g. change rooms and washrooms).
4. Recording equipment and storage devices must be in a strictly controlled access area. Only authorized personnel shall have access to the controlled access area and the recording equipment.
5. The annual maintenance program for recording equipment will ensure that the equipment is operating properly. Library staff will promptly follow-up issues or concerns regarding the performance of equipment.
6. 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 and/or unauthorized staff to view them.
7. The Library will take all reasonable efforts to ensure the security of records in its control/custody and ensure their safe and secure disposal.
8. Security camera systems will be set-up to ensure regular recordings are cleared or overwritten on a regular basis, typically every 30 days. In some cases, system capacity may limit the time records are maintained. If authorized staff need to remove information from the system (still images, video footage) for authorized reasons, the resulting record(s) will be maintained for at least one (1) year.

Notice of Use of Video Cameras

To provide notice to individuals that video is in use, the Library shall post signs at entrances and/or on the perimeter of the area(s) under video surveillance. Notice of security camera use will also be included on the Library's website. The notification requirements of this sign must satisfy the notification requirements under section 29(2) of MFIPPA, which includes:

1. The legal authority for the collection of personal information.
2. The principle purpose(s) for which the personal information is intended to be used.
3. The title, business address, and telephone number of someone who can answer questions about the collection.

Use of Video Recordings

Recorded material will only be used for the purposes defined by this Policy and in accordance with MFIPPA and associated procedures. The information collected through video surveillance is used only:

1. To provide law enforcement agencies with evidence related to an incident under investigation.
2. To investigate a critical bodily injury as defined by and reported to the Ministry of Labour.
3. To respond to a request for information under MFIPPA.
4. To aid in the investigation of an insurance claim.
5. To aid in the deterrence of improper or unlawful conduct by the public and staff.
6. To aid in the investigation into violations of BPL's Human Rights Policy or Violence in the Workplace Policy.

Access to Video Recordings

Access to video recordings is limited to:

1. Individuals responsible for the operation or administration of the system.
2. Individuals who have a legitimate need to access the information for one of the purposes indicated in this policy.
3. Individuals whose request for access under MFIPPA, as amended, has been granted.

Requests to View Video Records

All requests to view security camera footage will be directed to the CEO or designate for consideration and recorded in the log. Decisions to grant access will be based on Library policy and relevant legislation including MFIPPA. If access to video records is granted, the CEO or designate will provide the recording for the specified date and time of the incident in the approved request. Where possible, the release of information about individuals deemed not to be involved in the approved request will be limited. This includes, but is not limited to, zooming images in on approved footage in question, obscuring identifiable features of other individuals and limiting the time frame of video coverage provided.

Log

A Log will be kept of all instances of access to, and use of, recorded material to enable a proper audit trail. Logs will include all relevant details such as system maintenance, staff name, date, time, details of person requesting the information and reason for access to the records as well as specifics of the recording in question such as date, time, and location. Where the request is made by law enforcement, the name and badge number of the officer along with the investigation number will also be included.

Unauthorized Access and/or Disclosure (Privacy Breach)

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. The following actions will be taken immediately:

1. Upon confirmation of the existence of a privacy breach, the CEO or designate will notify the Information and Privacy Commission of Ontario (IPC).
2. BPL staff shall 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.
3. 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.
4. The staff member shall work with the departmental Director and the CEO or designate to take all reasonable actions to recover the record and limit the record's disclosure.
5. The CEO or designate where required, shall notify affected parties whose personal information was inappropriately disclosed.
6. 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.

Appendices

- Appendix 1: References

Appendix 1: References

- [Kingston Frontenac Public Library Video Surveillance Policy](#)
- [Barrie Public Library Video Surveillance Policy](#)
- [Hamilton Public Library Security Camera Policy](#)
- [IPC Privacy Fact Sheet – Disclosure of Personal Information to Law Enforcement](#)

Effective Date: October 15, 2020

Projected Review Date: October 2023

Motion #/Date: #20 -78

Amended Dates:

Associated Procedures: Protection of Customer Privacy Policy; Employee Code of Conduct Policy