Guelph Public Library
Explore • Connect • Thrive

Policy Type: **Operational** Policy Number: **OP- 17**

Video Surveillance

It is the policy of the Guelph Public Library 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.

1 Underlying Principles

1.1 In the daily operation of Guelph Public Library (GPL) premises, the safety of property, visitors, and employees is protected and maintained by conventional means such as: alert observation by staff, foot patrols by security personnel, security-conscious design of Library locations, safe behaviour training, and the consistent application of the Library's Standards of Acceptable Behaviour. However, in some circumstances, the additional protection provided by surveillance cameras is essential in maintaining lawful and safe use of Library premises.

1.2 The Video Surveillance Policy provides 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 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.

2 Policy Statement

Guelph Public Library recognizes the need to balance an individual's right to privacy and the need to ensure the safety and security of Library employees, clients, visitors and property. Proper video surveillance, where deemed necessary, is one of the most effective means of helping to keep Library facilities and properties operating in a safe and secure manner. While video surveillance cameras are installed for safety and security reasons, the Library's video surveillance systems must be designed and maintained to minimize privacy intrusion.

3 Scope

This Policy applies to all types of camera surveillance systems, surveillance monitors and camera recording devices that are used for security purposes at Library-owned and leased properties. This Policy does not apply to video surveillance used for employment-related or labour-related information.

4 Application

This Policy applies to the Guelph Public Library staff, Library contractors and service providers who have responsibilities relating to security video surveillance. They will be made aware of this Policy and given instruction in meeting the policy's requirements.

5 Specific Directives

5.1 Designing and Installing Video Surveillance Equipment

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

a. 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 video surveillance systems may operate at any time in a 24-hour period;

b. The video equipment shall be installed to monitor only those spaces that have been identified as requiring video surveillance;

c. 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 video surveillance program;

d. 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);

e. 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;

f. Every reasonable attempt should be made by authorized personnel to ensure video monitors are not in a position that enables the public and/or unauthorized staff to view the monitors.

6 Notice of Use of Video Systems

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

a. The Library shall post signs, visible to members of the public, at all entrances and/or prominently displayed on the perimeter of the grounds;
b. The notification requirements of this sign must inform individuals of:
    i. The legal authority for the collection of personal information;
    ii. The principal purpose(s) for which the personal information is intended to be used; and
    iii. The title, business address, and telephone number of someone who can answer questions about the collection.

7 Personnel Authorized to Operate Video Equipment

Only employees designated by the Chief Executive Officer shall be permitted to operate video surveillance systems.

8 Video Equipment/ Recordings

8.1 Types of Recording Device

The Library use Digital Video Recorders (DVR) in its video systems. Facilities using video recorders will retain these records for a period of up to 30 days. A record of an incident will only be stored longer than 30 days where it may be required as part of a criminal, safety, or security investigation or for evidentiary purposes.

8.2 Recording Identification

In facilities with a DVR that stores information directly on a hard-drive, the camera name, computer time and date stamp shall be understood to be its identification label.

8.3 Logbook

A logbook shall be maintained to record all activities related to video devices 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 and activity. This logbook must remain in a safe and secure location. Only personnel authorized by the CEO may remove this logbook from the secure location.

9 Access to Video Recordings

9.1 Storage

All storage devices that are not in use must be stored securely in a locked receptacle located in an access-controlled area.

9.2 Formal Access Requests Process

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

9.3 Viewing Video

When recorded video 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.

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

9.4.1 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 from access or use of information from the video surveillance system, its components, files, or database for personal reasons.

9.4.2 Video that has not been formally requested within the maximum retention period is considered transitory and is automatically erased by being overwritten. Library facilities use DVR equipment to store information until the storage capacity of the hard drive has been reached at which time the video is overwritten.

9.4.3 The Library will take all reasonable efforts to ensure the security of records in its control/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.

9.5 Unauthorized Access and/or Disclosure (Privacy Breach)

9.5.1 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 is immediately informed of the breach.

9.5.2 A breach is any unauthorized or illegal collection, use, or disclosure of personal information. In the event of a breach the CEO or designate will:

a. Contain the breach and repatriate the information.

b. Assess the severity of the breach.

c. Notify affected parties and the Information and Privacy Commissioner as required.

d. Investigate the cause of the breach.

e. Implement corrective actions.

9.5.3 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.

9.6 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.

10 Accountability

The CEO:

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

b. Will report to the Board when video surveillance is being proposed for any location;

c. Providing advice, training and recommendations to staff to assist in compliance with MFIPPA;

d. Undertaking yearly evaluation of GPL's video surveillance systems to ensure compliance with this Policy;

e. Ensuring training in compliance with this Policy is available and provided to appropriate staff and service providers;

f. Responding to formal requests to access records, including law enforcement inquiries;

g. Investigating privacy complaints related to video surveillance records, and security/privacy breaches.

References

Guidelines for the Use of Video Surveillance Cameras in Public Places. Information and Privacy Commissioner/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.