Policy Type: Operational

Policy No: OP-04

Policy Title: Security Camera Policy

Effective: March 22, 2023

Review Date: March 2026

The Grey Highlands Public Library Board strives to maintain a safe and secure environment for staff and members of the public while protecting individual rights to privacy. Security cameras assist in achieving this goal. This policy follows the privacy requirements set out in the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the guidelines set out by the Information and Privacy Commission of Ontario.

Section 1: General

This policy is meant to assist the Board and staff in their goal of maintaining safe Library facilities, while protecting individual rights to privacy. The CEO will issue administrative procedures to staff in support of this policy.

Section 2: Application

This policy applies to all facilities with security cameras operated by the Grey Highlands Public Library Board. This policy does not address instances where staff may video record for an event, program, or presentation on behalf of the Library of Grey Highlands Cultural Channel.

Section 3: Responsibilities

The CEO, Digital Services/Branch Manager, or other designated employees are authorized to operate the systems. Library employees and service providers are to review and comply with the Policy, Guidelines, and relevant legislation in performing their duties and functions related to the operation of the video surveillance system.

CEO – The CEO is responsible for the overall Library video security surveillance program and is responsible for the Library's privacy obligations under MFIPPA, R.S.O. 1990 c. M. 56 and this policy.

Digital Services/Branch Manager – The Digital Services/Branch Manager is responsible for the technical aspects of the equipment, including the installation,

retention, and disposal of the recorded information.

The Library Board – The Library Board, through their designate, is responsible for the development and review of the policy and supporting guidelines.

All staff – All staff are responsible for adhering to the guidelines outlined in this policy, and direction/guidance that may be given to them from time-to-time regarding monitoring of security cameras and directing community questions/requests to the CEO.

Section 4: Collection of Personal Information Using a Video Surveillance System

Any recorded data of an identifiable individual qualifies as "personal information" under MFIPPA. Security cameras can be used to collect personal information about identifiable individuals. The Library has determined that it has the authority to collect this personal information in accordance with the MFIPPA. Pursuant to section 28(2) of the MFIPPA, no person shall collect personal information on behalf of the Library unless the collection is expressly authorized, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

Before deciding if a facility warrants video surveillance, the Library will:

1. Only consider video surveillance where there is evidence that staff patrols have proven to be unworkable or ineffective.
2. Be able to demonstrate that:
    a. There is a history of incidents occurring in the specific facility.
    b. That video surveillance would prevent future incidents from occurring; and
    c. That surveillance would increase the overall safety of staff, public, and facility.
3. Endeavour to ensure that the proposed video security system minimizes privacy intrusion to that which is necessary to achieve its required lawful goals.

Section 5: Design, Installation, and Operation of Video Surveillance Equipment

In designing, installing, and operating a video security surveillance system, the Library will consider:

1. Cameras that operate 24 hours/seven days a week, within the limitations of system capabilities, power disruptions, and serviceability/maintenance.
2. Cameras that are positioned in a way that surveils Library property. They will not be positioned to look through the windows of adjacent buildings.
3. Clearly written signs that provide staff and the public with a warning that video surveillance is in effect. Signage will satisfy the notification requirements under section 29(2) of MFIPPA, R.S.O. 1990, c. M. 56, which include

informing 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.

4. Ensuring that video monitors are not in the position of public viewing.
5. Maintenance of the equipment and promptly following up with issues and concerns regarding the performance of the equipment.
6. That equipment shall never monitor the inside of areas where the public and employees have a higher expectation of privacy (e.g. washrooms).
7. That the Security Camera Policy be posted on the Library's website.

While security camera footage is not used to actively monitor employee performance, where warranted, camera footage may be reviewed and/or monitored for workplace investigation purposes such as policy violations, health and safety concerns, crime, and/or theft. The aforementioned works in conjunction with the Grey Highlands Public Library's Privacy Policy and Section 5.3 of the Employee Handbook, which should be consulted together with the contents of this section.

Section 6: Access, Use, Disclosure, Retention, Security and Disposal of Video Security Surveillance Records

Security camera footage may only be used for the purposes set out in the policy and must relate to the protection of clients, staff, the public, and the facility. Information should not be retained or used for any purposes other than those described in the policy. Circumstances which warrant review will be limited to security incidents that have been reported, or in the 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.

Each facility having a system will implement the following procedures:

1. Storage of footage will be kept in a secure area. Logs should be kept of all instances, access to, and use of, recorded material to enable a proper audit trail.
2. Only the CEO, Branch Managers, or other authorized delegates may review the information. Circumstances, which would warrant review, will normally be limited to an incident that has been reported/observed or to investigate a potential crime. Real-time viewing may be delegated by the CEO to a limited number of individuals.
3. Video may be disclosed to the police when:
    a. Law enforcement approaches the Library with a warrant requiring the disclosure of footage; as per section 42(1)(e) of FIPPA and section 32(g)

of MFIPPA; or

b. You observe an illegal activity on your premises and disclose the footage to a law enforcement agency to aid an investigation from which a proceeding is likely to result, as per section 42(1)(g) of FIPPA and section 32 (g) of MFIPPA.

4. The retention period for information that has not been viewed for law enforcement, Library, or public safety purposes shall be a minimum of 5 days but not exceed 30 calendar days for digital systems. These time-frames are based on risk assessment, privacy considerations, and equipment capabilities. Recorded information that has not been used in this fashion, within these time-frames, is then routinely erased in a manner in which it cannot be reconstructed or retrieved.
5. When recorded information has been viewed for law enforcement, facility, or public safety purposes, the retention period shall be one year from the date of viewing as per Section 5 of the Ontario Regulation 823 of MFIPPA.
6. The Library will store and retain storage devices required for evidentiary purposes according to standard procedures until the law enforcement authorities request them. A release form will be completed before any storage device is disclosed to appropriate authorities. The form will indicate who took the device, under what authorities, when this occurred, and if it will be returned or destroyed after use. This activity will be subject to audit.
7. Old storage devices must be securely disposed of in such a way that personal information cannot be reconstructed or retrieved. Disposal methods could include shredding, burning or magnetically erasing personal information. A record of the disposal is to be completed and retained.
8. Any patron, Staff Member or member of the public who has been recorded by a video security surveillance camera has a general right of access to his or her personal information under section 36 of MFIPPA, R.S.O. 1990, c. M. 56. This right is recognized. One exemption that may apply is contained in subsection 38(b) of MFIPPA, R.S.O. 1990, c. M. 56, which grants the heads of an institution the discretionary power to refuse access where disclosure would constitute an unjustified invasion of another individual's privacy. As such, access to an individual's own personal information in these circumstances may depend upon whether any exempt information can be reasonably severed from the record. One way in which this may be achieved is through digitally "blacking out" the images, where technically possible, of other individuals whose images appear on the recording(s).
9. The application of the frivolous or vexatious request provisions of MFIPPA, R.S.O. 1990, c. M. 56, would occur in very rare circumstances. It can be concluded that a request for access to a record or personal information is frivolous or vexatious if: a) The opinion is, on reasonable grounds, that the request is part of a pattern of conduct that amounts to an abuse of the right of access or would interfere with the operations of the facility, or b) The opinion is, on reasonable grounds, that the request is made in bad faith or for a purpose

other than to obtain access.

10. The CEO will respond to any inadvertent disclosures of personal information. Any breach of Ontario's Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M. 56, shall be reported to the CEO.

Section 7: Training

Where applicable and appropriate, the policy and guidelines will be incorporated into training and orientation programs of the Library Staff. Training programs addressing staff obligations under the MFIPPA shall be conducted as necessary.

Section 8: Auditing and Evaluating the use of a Video Surveillance System

The Library will ensure that the use and security of video security surveillance equipment is subject to regular audits. The audit will address the Library's operational compliance with the policy and the guidelines. An external body may be retained to perform the audit. The Library will endeavour to address any deficiencies or concerns identified by the audit as soon as possible. Employees and service providers should be aware that their activities are subject to audit and that they may be called upon to justify their surveillance interest in any given individual. The Library will regularly review and evaluate its video surveillance program to ascertain whether it is still justified in accordance with the planning requirements set out in this document. This evaluation shall occur at least once every three years and will include the review/update of the policy and the guidelines.

Definitions

Personal Information (taken from MFIPPA): Recorded information about an identifiable individual, including:

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except if they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(h) the individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

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.

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.

Related Documents:

Municipal Freedom of Information and Protection of Privacy Act
Information and Privacy Commission of Ontario