Huntsville Public Library

Security & Video Surveillance Policy

Policy Number: 18-00
Policy Approval Date: October 9, 2018
Policy Review Date: October 2021

Definitions

Access Request: a formal request for access to records made under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

Act: the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

Disclosure: refers to the release of relevant information. Disclosure includes viewing recordings or images, as well as making copies of recordings or images.

The CEO/Chief Librarian is the Freedom of Information/Privacy Officer for Huntsville Public Library.

HPL or Library: the Huntsville Public Library or, if the context so requires, any premises used by the Huntsville Public Library for Library purposes.

Production Order: requires the custodian of documents to deliver or make available the documents to persons such as law enforcement officials within a specified period.

Library Security: means a person or team of people contracted by Huntsville Public Library to provide security services in the Library.

Personal information: (as defined by MFIPPA) is recorded or unrecorded information about an identifiable individual, including but not limited to:

1. Information relating to race, national or ethnic origin, religion, age, sex, sexual orientation or marital or family status of the individual.
2. 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.
3. Any identifying number, symbol or other particular assigned to the individual.
4. The address, telephone number, fingerprints or blood type of the individual.
5. The personal opinions or views of the individual except if they relate to another individual.
6. 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.

7. The views or opinions of another individual about the individual.
8. 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.

Record: any record of information however recorded, whether in printed form, on film, by electronic means for otherwise:

1. Correspondence, a memorandum, a book, a plan a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape or DVD, a machine readable record, any other documentary material.
2. Subject to the regulations, any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution.

Retention Period: the period of time during which specific records series must be kept before records in that records series may be disposed of.

Staff: refers to individuals employed by Huntsville Public Library Board for wages or salary. For clarity, this term includes support staff, management and professional staff.

Service Provider: means a video service provider, consultant or other contractor engaged by the Town in respect of the video surveillance system

Storage Device: a videotape, computer disk or drive, CD, computer chip or other device used to store the recorded data or visual, audio or other images captured by a video surveillance system

Video Surveillance System: a video, physical or other mechanical, electronic, digital or wireless surveillance system or device that enables continuous or periodic video recording, observing or monitoring of information about individuals in open, public spaces. In this policy, the term video surveillance system includes an audio device, thermal imaging technology or any other component associated with capturing the image of an individual.

Scope

This policy applies to all Library Employees, members of the Library Board and Service Providers.

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

This policy does not address instances where library staff records a specific event (such as a programme, or presentation).

This policy does not apply to covert surveillance used as an investigation tool for law enforcement purposes or in contemplation of litigation.

Policy

Security camera systems are a resource used by the Huntsville Public Library Board within the Board's jurisdiction to promote the safety of users, staff and community members. Where deployed for that purpose, these systems also help to protect Library property against theft or vandalism and can assist in the identification of intruders and of persons breaking the law.

In the event of a reported or observed incident, the review of recorded information may be used to assist in the investigation of the incident. The Library will maintain control of and responsibility for the security camera system at all times. Library staff and service providers are expected to review and comply with this Policy, the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), and other relevant statutes in performing any duties and functions that are related to the operation of the security camera program.

Collection of Personal Information Using a Security Camera Coverage 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 Ontario 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.

Planning Considerations for Security Cameras

Before deciding if a facility warrants security cameras, the Library will:

1. Conduct consultations with relevant stakeholders as to the necessity of the proposed security camera program at the facility.
2. Endeavour to ensure that the proposed design and operation of the video security surveillance system reasonably minimizes privacy intrusion.

Design, Installation and Operation of Security Cameras

Prior to the installation of a video surveillance system at the Library, the eLibrarian and CEO/Chief Librarian (Freedom of Information/Privacy Officer) will:

1. Identify relevant stakeholders
2. Consult with relevant stakeholders and provide them with the opportunity to comment on the specifics of the proposed installation, for example the location of the video surveillance system as well as the use of the system.
3. Justify the use of the new video surveillance system on the basis of quantified reports of incidents or public or employee safety or unlawful activities. The CEO/Chief Librarian will:
    a. Conduct a video surveillance PIA to evaluate the privacy impact of the installation of a video surveillance system; and
    b. Ensure that the objectives and sage of the proposed new video surveillance system are consistent with the IPC's Guidelines for the Use of Video Surveillance Cameras in Public Spaces.

Notification of the Public

The Library will ensure that the public is notified about the presence of video surveillance equipment, whether recording or for surveillance purposes, by prominently posting signs at the perimeter of surveillance areas.

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

1. 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 security camera coverage. On at least one sign at each location with security camera coverage the following information will included:

    a. The legal authority for the collection of personal information;

    b. The principle purpose(s) for which the personal information is intended to be used;

    c. The title, business address, and telephone number of someone who can answer questions about the collection.

2. Additional signs will be used to support awareness of the security camera program.
3. Access to this policy on the Virtual Library (www.huntsvillelibrary.ca).

Security Camera Monitors, Records and Retention

1. Only the CEO/Chief Librarian or designate may review recorded information from the system.

2. Security camera footage will not be used to monitor users' use of Library spaces or staff performance. 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.
3. All storage devices will be located in a controlled-access area. Access to the storage devices will be limited to authorized personnel. Logs will be kept of all instances of access to, and use of, recorded material to enable a proper audit trail.
4. The Library will take all reasonable efforts to ensure the security of records in its control/custody and ensure their safe and secure disposal.
5. Security camera systems will be set-up to ensure regular recordings are cleared or overwritten on a regular basis. Normally, systems will be set-up to maintain records for up-to 30 days. In some cases system capacity may limit the time records are maintained. In the event that 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 and 30 days from the date of receipt of an application.
6. When records are released to law enforcement officials, where possible, the CEO/Chief Librarian will limit the release of information about individuals deemed not to be involved in the investigation. This includes, but is not limited to, zooming images in on suspects in question, obscuring identifiable features of other individuals and limiting the time frame of video coverage provided.

Logs

Each facility must maintain a log at a secure location that records all activities related to security cameras 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.

Access Requests Process

All requests to view security camera coverage will be recorded in the Log and will be directed to the CEO/Chief Librarian. Requests will be reviewed based on Library policy and relevant legislation including MFIPPA.

Law Enforcement Access Request

If access to a video surveillance record is required for the purpose of a law enforcement investigation, the requesting officer must complete the "Law Enforcement Request Form" (Appendix A). Law enforcement agencies may include but are not limited to:

1. Ontario Provincial Police
2. Royal Canadian Mounted Police
3. Municipal Police Force

Personal Information Requests
An individual whose personal information has been collected by a video surveillance system has a right of access to his or her personal information under section 36 of the MFIPPA.

1. All requests for video records will follow the Freedom of Information (FOI) request process as outlined in MFIPPA.
2. Access to personal information may depend on whether there is an unjustified invasion of another individual's privacy and whether any exempt information can be reasonably severed from the record.
3. The Freedom of Information Officer may charge fees for this service in accordance with MFIPPA.

The CEO/Chief Librarian, or designate, will record the following information in the facility's log:

1. The name of the Officer and badge number
2. Investigation number and reason for the request
3. The date and time of the original, recorded incident including the designated name/number of the applicable camera and DVR
4. The name of the authorized personnel at the time of the incident
5. The time and date the copy of the original record was sealed
6. The time and date the sealed record was provided to the requesting Officer
7. Whether 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 for investigative reasons, this must only be undertaken by the CEO/Chief Librarian, in a private, controlled area that is not accessible to other staff and/or visitors.

Inquiries from the Public Related to the Security Camera Coverage Policy

A staff member receiving an inquiry from the public regarding the Security camera coverage Policy shall direct the inquiry to the CEO/Chief Librarian.

Accountability - Roles & Responsibilities

CEO/Chief Librarian - The CEO/Chief Librarian is responsible for the overall Library security and video surveillance program and is responsible for the Library's privacy obligations under the Ontario Municipal Freedom of Information and Protection of Privacy Act and the Policy and will prepare annual reports to the Board on the security camera program. Only the Chief Librarian and specifically designated staff will have the

authority to review recorded camera coverage and authorize the release of images from the system for investigations or other purposes

Personnel Authorized to Operate Video Equipment

Only authorized personnel shall be permitted to operate security camera coverage systems.

Unauthorized Access and/or Disclosure (Privacy Breach)

Any Library staff 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/Chief Librarian is immediately informed of the breach.

The following actions will be taken immediately in accordance with HPL's procedures for managing a privacy breach:

- Upon confirmation of the existence of a privacy breach, the CEO/Chief Librarian or designate will notify the Information and Privacy Commission of Ontario (IPC).
- The CEO/Chief Librarian 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.
- The CEO/Chief Librarian shall investigate the cause of the disclosure with the goal of eliminating potential future occurrences.
- The CEO/Chief Librarian will be informed of events that have led up to the privacy breach.
- The staff member shall work with the CEO/Chief Librarian to take all reasonable actions to recover the record and limit the record's disclosure.
- The CEO/Chief Librarian, where required, shall notify affected parties whose personal information was inappropriately disclosed.
- 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.

The length of time for which recordings or images captured by the Video Surveillance System will be preserved is dependent upon the storage capacity of the Video Surveillance System and may be as little as three days. In cases in which the Library has received a request for Disclosure of recordings or images and has verified that the requested recordings or images exist, those recordings or images will be preserved for the period of time necessary to satisfy the Disclosure request.

RELATED DOCUMENTS & INFORMATION

Code of Conduct Policy

Guidelines for the Use of Video Surveillance (October 2015) | Information and Privacy Commissioner of Ontario
The Information and Privacy Commissioner/Ontario www.ipc.on.ca
Municipal Freedom of Information Act
Privacy Policy
Technology @ HPL Policy
Video Surveillance Administration Procedures

HISTORY
Motion 12-34; Revised & Adopted April 16, 2012.