

POLICY: SECURITY VIDEO SURVEILLANCE

**SECTION: Section V – Municipal Freedom of Information and
Protection of Privacy Act, R.S.O. 1990, c. M. 56**

MOTION#/DATE: 07 - – March 26, 2007

Effective Date

March 26, 2007

Table of Contents

Policy Objective	3
Underlying Principles	3
Policy Statement	3
Scope	3
Application	4
Specific Directives	4
A. Guidelines to Follow Prior to the Implementation of a Video Surveillance System	4
1. Factors to Consider Prior to Using Video	4
2. Designing and Installing Video Surveillance Equipment	4
3. Notice of use of Video Systems	5
4. Personnel Authorized to Operate Video Equipment	5
B. Video Equipment/Records	6
1. Types of Recording Device	6
2. Record Identification	6
3. Logbook	6

[Table of Contents, continued]

C.	Access to Video Records	6
1.	Access	6
2.	Storage	7
3.	Formal Access Requests Process	7
4.	Access: Law Enforcement	7
5.	Viewing Images	8
6.	Custody, Control, Retention and Disposal of Video Records/ Recordings	8
7.	Unauthorized Access and/or Disclosure (Privacy Breach)	8
8.	Inquiries from the Public Related to the Video Surveillance Policy	9
	Accountability	10
	Appendices	
	Appendix 1: References	12
	Appendix 2: Definitions	13
	Appendix 3: Contacts	14

Policy Objective

To ensure that, in adopting the use of security video surveillance cameras, Toronto Public Library balances the security benefits derived from the use of video surveillance with the privacy rights of the individual.

Underlying Principles

In the daily operation of Toronto Public Library (TPL) 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 Rules of Conduct. However, in some circumstances, the additional protection provided by surveillance cameras is essential in maintaining lawful and safe use of Library premises.

The Security Video Surveillance Policy provides detailed 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.

Policy Statement

Toronto 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.

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.

Application

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

Specific Directives

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

1. Factors to Consider Prior to Using Video

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

- (a) The use of video surveillance cameras should be justified on the basis of verifiable, specific reports of incidents of crime or significant safety concerns.
- (b) A video surveillance system should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable.
- (c) An assessment must be conducted on the effects that the proposed video surveillance may have on personal privacy, and the ways in which any adverse effects can be mitigated.
- (d) The proposed design and operation of the video surveillance systems should minimize privacy intrusion.

2. 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) Reception/recording equipment must be located in a strictly controlled access area. Only authorized personnel shall have access to the controlled access area and the reception/recording equipment.
- (g) 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.

3. Notice of Use of Video Systems

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 under video surveillance.
- (b) The notification requirements of this sign must inform individuals of:
 - (i) the legal authority for the collection of personal information;
 - (ii) the principle 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.

4. Personnel Authorized to Operate Video Equipment

Only authorized personnel shall be permitted to operate video surveillance systems.

B. Video Equipment/Records

1. Types of Recording Device

The Library may use either Digital Video Recorders (DVR) or time lapse Video Cassette Recorders (VCR's) in its video systems. Facilities using video recorders will retain these records for a period of up to 30 days depending on the recording device and technology. 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.

2. Record Identification

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 hard-drive, the computer time and date stamp shall be understood to be this identification. In facilities with a VCR or other recording mechanism using a removable/portable storage device, the authorized personnel shall affix a label to each storage device identifying this information.

3. Logbook

Each location shall maintain a logbook 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 with the video recording equipment. Only authorized personnel or a manager may remove this logbook from the secure location.

C. Access to Video Records

1. Access

Access to the video surveillance records, e.g. logbook entries, CD, video tapes, etc. shall be restricted to authorized personnel, and only in order to

comply with their roles and responsibilities as outlined in the Security Video Surveillance Policy.

2. Storage

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

3. Formal Access Requests Process

With the exception of requests by law enforcement agencies, all formal requests for video records should be directed to the City Librarian's office. Requests are subject to the requirements of the Library's Access to Information and Protection of Privacy Policy.

4. Access: Law Enforcement

If access to a video surveillance record is required for the purpose of a law enforcement investigation, the requesting Officer must complete the Disclosure of Personal Information Form and forward it to the City Librarian, or designate. The City Librarian or designate will provide the recording for the specified date and time of the incident requested by the Law Enforcement Officer, subject to MFIPPA exemptions.

The City 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 VCR/DVR;
- (ii) The name of the authorized personnel at the time of the incident;
- (iii) The time and date the copy of the original record was sealed;
- (iv) The time and date the sealed record was provided to the requesting Officer; and,
- (v) Whether the record will be returned or destroyed after use by the Law Enforcement Agency.

5. Viewing Images

When recorded images from the cameras must be viewed for law enforcement or investigative reasons, this must only be undertaken by an authorized personnel, in a private, controlled area that is not accessible to other staff and/or visitors.

6. Custody, Control, Retention and Disposal of Video Records/Recordings

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.

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/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.

7. Unauthorized Access and/or Disclosure (Privacy Breach)

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 City Librarian is immediately informed of the breach.

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

- Upon confirmation of the existence of a privacy breach, the City Librarian or designate will notify the Information and Privacy Commission of Ontario (IPC).
- TPL 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.
- The City Librarian, 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.
- The departmental Director shall inform the City Librarian, or designate, of events that have led up to the privacy breach.
- The staff member shall work with the departmental Director and the City Librarian, or designate to take all reasonable actions to recover the record and limit the record's disclosure.
- The City 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.

8. 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 City Librarian's Office.

Accountability

1. The City Librarian:
 - (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 locations where there is a high-profile public presence.
 - (c) Preparing annual reports to the Board on all security video surveillance systems installed.

2. Directors are responsible for:
 - (a) Approving proposed installations in their department after a Security Threat Assessment has been completed.
 - (b) Recommending to the City Librarian any proposed installation in their department which should be considered as high-profile, and therefore reported to the Board.

3. The Director, Corporate and Service Planning, Policy, Projects and City-wide Services is responsible for:
 - (c) Providing advice, training and recommendations to staff to assist in compliance with MFIPPA
 - (d) Undertaking yearly evaluation of TPL's video surveillance systems to ensure compliance with this Policy
 - (e) Reviewing this Policy every two years, and recommending updates as appropriate to the City Librarian.
 - (f) Ensuring training in compliance with this Policy is available and provided to appropriate staff and service providers.And, in consultation with the City Librarian, for:
 - (g) Responding to formal requests to access records, including law enforcement inquiries
 - (h) Investigating privacy complaints related to video surveillance records, and security/privacy breaches

4. The Director, Information Technology and Facilities, or designate, is responsible for:
 - (a) Conducting Security Threat Assessments to determine requirement for a video surveillance system.
 - (b) Advising on installations and operation.

- (c) Assessing proposed installations in accordance with this Policy in consultation with the appropriate director.
 - (d) Conducting periodic internal audits to ensure compliance with this Policy.
 - (e) Delegating the day-to-day operations of video surveillance systems to managers, and ensuring system-wide compliance with this Policy and TPL procedures.
 - (f) Ensuring that appropriate Facilities staff are familiar with this Policy, and that training is provided to all authorized personnel.
5. Library Service Managers, and Facilities' Managers at Toronto Reference Library, are responsible for
- (a) Complying with this Policy.
 - (b) 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.
 - (c) Ensuring that training is provided to the authorized personnel and the authorized staff they supervise.
 - (d) Ensuring that all the staff they supervise are familiar with this Policy.
 - (e) Ensuring monitoring and recording devices, and all items related to surveillance (e.g. logbooks) are stored in a safe and secure location.
 - (f) Ensuring logbooks recording all activities related to security video devices and records are kept and maintained accurately by authorized personnel.
 - (g) Informing appropriate shared facilities' personnel of this Policy's requirements.
 - (h) Immediately reporting breaches of security/privacy to the City Librarian or designate.

Appendices

Appendix 1: References

Appendix 2: Definitions

Appendix 3: Contacts

Appendix 1

References

Guidelines for Using Video Surveillance Cameras in Public Places. Information and Privacy Commissioner/Ontario. 2001.

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.

Toronto Public Library Access to Information and Protection of Privacy Policy.

Appendix 2

Definitions

Authorized staff/personnel – employees of TPL or of a TPL contractor who are authorized by the Library to operate the video surveillance system for a particular facility and to perform the duty, responsibility or action described.

Appendix 3

Contacts

City Librarian's Office: Privacy breaches.

Director, Corporate and Service Planning, Policy, Projects, and City-Wide Services: Compliance with MFIPPA; formal requests to access records, including law enforcement inquiries; complaints.

Director, Information Technology and Facilities: Installation, management and operation of security video surveillance systems.