BRANTFORD PUBLIC LIBRARY

Policy Title: Video Surveillance Policy	**Policy Number:** FAC 06
Policy Type: Operational	**Policy Category:** Facilities
Date Created: December 2012	**Date Approved:**
Chair/CEO Signature:	
Supersedes:	**Date Revised/Amended:**
Background documents, related policies:	
Author:	

Policy Statement:

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

Policy Description:

This Library policy has been developed to govern video surveillance at existing and future Library Branches in accordance with the privacy provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

Application:

This policy applies to all types of camera surveillance systems, surveillance monitors and camera recording devices at Library Branches that are used for security purposes. This policy does not apply to the "People Counter" used at the Libraries.

Responsibilities:

The Chief Executive Officer is responsible for the Video Surveillance Policy.

Roles and Responsibilities:

Responsibilities of Chief Executive Officer:

The Chief Executive Officer may delegate various responsibilities under this Policy to Managers. The key duties of the Chief Executive Officer include:

- Is responsible and accountable for documenting, implementing, enforcing, monitoring and updating the Library's privacy and access compliance;
- Will report to the Board when video surveillance is being proposed for all locations; Preparing annual reports to the Board on all security video surveillance systems installed.
- Informing appropriate shared facilities' personnel of this Policy's requirements if in a shared facility;

Managers

Managers are responsible for:

- Recommending proposed installations in their department after reviewing Security Threat Assessments;
- Ensuring that appropriate library staff are familiar with this Policy and providing advice, training and recommendations to staff to assist in compliance with MFIPPA;
- 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;
- Ensuring monitoring and recording devices, and all items related to surveillance (e.g. logbooks) are stored in a safe and secure location;
- Ensuring logbooks recording all activities related to security video devices and records are kept and maintained accurately by authorized personnel;
- Responding to formal requests to access records, including law enforcement inquiries, in consultation with the Chief Executive Officer or designate;
- Investigating privacy complaints related to video surveillance records, and security/privacy breaches.
- Immediately reporting breaches of security/privacy to the Chief Executive Officer or designate.
- Reviewing annually the video surveillance system and policy and recommending updates as appropriate to the Chief Executive Officer;

Responsibilities of Manager, Business Services

The Manager, Business Services as designated by the Chief Executive Officer shall:

- Reviewing Security Threat Assessments to determine requirement for a video surveillance system;
- Advising on installations and operation;
- Assessing proposed installations in accordance with this Policy in consultation with the appropriate manager;
- Conducting periodic internal audits to ensure compliance with this Policy;
- Delegating the day-to-day operations of video surveillance systems to managers and ensuring compliance with this Policy and BPL procedures;

The IT Department Staff

The IT Department staff are responsible for:

(a) Technical aspects of equipment, its installation and maintenance and the retention and disposal of the recorded information.

Responsibilities of All Library Staff

All Library Staff must adhere to the video surveillance policy and must not access or use information contained in the video surveillance system, it's components, files, or database for personal reasons, nor dispose, destroy, erase or alter any record without proper authorization and without following the regulations contained in the Security Video Surveillance Policy.

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

Factors to Consider Prior to Using Video

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

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

Designing and Installing Video Surveillance Equipment

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

- Given the open and public nature of the Library's facilities and the need to provide for the safety and security of employees and clients 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.
- The video equipment should be installed to only monitor those spaces that have been identified as requiring video surveillance.
- The ability to adjust cameras should be restricted, if possible, so that cameras cannot be adjusted or manipulated to overlook spaces that are not intended to be covered by the video surveillance program.
- Equipment should never monitor the inside of areas where the public and employees have a higher expectation of privacy (e.g. change rooms and washrooms).
- Where possible, video surveillance should be restricting to periods when there is a demonstrably higher likelihood of crime being committed and detected in the area under surveillance.

- Reception/recording equipment must be located in a strictly controlled access area. Only designated staff, or those properly authorized in writing by the DDM, shall have access to the controlled access area and the reception/recording equipment.
- Every reasonable attempt should be made to ensure video monitors are not in a position that enables the public and/or unauthorized staff to view the monitors.

***Notice of Use of Video* Systems**

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

- 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.
- The notification requirements of this sign must inform 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.

Personnel Authorized to Operate Video Equipment

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

Video Equipment I Records Types of Recording Devices

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

Record Identification Logbook

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 harddrive, the computer time and date stamp shall be understood to be this identification.

A logbook shall be maintained to record all activities related to video devices and records. The activities include all information regarding the use, maintenance, and storage of records and all instances of access to, and use of, recorded material. All logbook entries will detail authorized staff, date, time and activity. This logbook must remain in a safe and secure location with the video recording equipment. Only the Chief Executive Officer or Managers are authorized to remove this logbook from the secure location.

Access to Video Records

Access to the video surveillance records, e.g. logbook entries, CD, video tapes, etc shall be restricted to authorized personnel only in order to comply with their roles and responsibilities as outlined in the Video Surveillance Policy.

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.

Formal Access Requests Process

All requests for video records should be directed to the Chief Executive Officer or designate for processing. A person requesting access to a record should make a request in writing either in the form of a letter or the prescribed form (See Appendix #2: Access/ Correction Form) and submit it to the Chief Executive Officer. The individual requesting the record must:

- Provide sufficient detail (the approximate time and date, the location - if known - of the incident, etc.) to enable an experienced employee of the Brantford Public Library, upon a reasonable effort, to identify the record; and,
- At the time of making the request, pay the prescribed fees as provided for under the Act.

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 Library's Law Enforcement Officer Request Form (See Appendix #1) and forward this form to the Chief Executive Officer or designate. The Chief Executive Officer, or designate, will provide the recording for the specified date and time of the incident as requested by the Law Enforcement Officer. The Chief Executive Officer, 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 Operator 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. if 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 or investigative reasons, this must only be completed by an individual(s) authorized by the Chief Executive Officer in a private, controlled area that is not accessible to other staff and/or visitors.

Custody, Control, Retention and Disposal of Video Records I Recordings

The Brantford Public 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 the MFIPPA, which includes but is not limited to the prohibition of all Library

Staff from access or use of information from the video surveillance system, it's 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.

Unauthorized Access and/or Disclosure (Privacy Breach)

Library staff who become aware of any unauthorized disclosure of a video record in contravention of this Policy and/or a potential privacy breach are to immediately notify the Chief Executive Officer. After this unauthorized disclosure or potential privacy breach is reported:

- Upon confirmation of the existence of a privacy breach, the Chief Executive Officer shall notify the Information and Privacy Officer of Ontario (IPC) and 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 Chief Executive Officer work with the Manager, Business Services to take all reasonable actions to recover the record and limit the record's disclosure.
- The Chief Executive Officer, in consultation with the Manager, Business Services, and where required, will notify affected parties whose personal information was inappropriately disclosed.
- The Chief Executive Officer, in consultation with the Manager, Business Services shall investigate the cause of the disclosure with the goal of eliminating potential future occurrences. Intentional wrongful disclosure, or disclosure caused by negligence, by employees of the Library may result in disciplinary action up to and including dismissal. Intentional wrongful disclosure, or disclosure caused by negligence, by service providers (contractors) to the Library, may result in termination of their contract.

Inquires 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 Chief Executive Officer.

Review of Video Surveillance Policy

This policy shall be reviewed every 2 (two) years by the Chief Executive Officer who will forward recommendations for update, if any, to the Brantford Public Library Board for approval.