Board Policy
Security Video Surveillance

Security Video Surveillance

The purpose of this policy is to recognize the need to balance an individual's right to privacy and the need to ensure the safety and security of Library employees, customers, visitors and property. Proper video surveillance, where deemed necessary, can be an 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.

Specific Directives

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.

Personnel Authorized to Operate Video Equipment

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

Video Equipment/Records

Retention period

Facilities using video recorders will retain these records for a period of up to 3 days depending on the recording device and technology.

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.

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.

Policy Approved: June 2010

Board Policy
Security Video Surveillance

Access to Video Records

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.

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

With the exception of requests by law enforcement agencies, all formal requests for video records should be directed to the Executive Director's office. Requests are subject to the requirements of the Library's Privacy Policy.

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 a Disclosure of Personal Information Form and forward it to the Executive Director, or designate. The Executive Director or designate will provide the recording for the specified date and time of the incident requested by the Law Enforcement Officer, subject to FOIPP exemptions.

Viewing Images

When recorded images 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.

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 FOIPP, 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.

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.

Policy Approved: June 2010

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 Executive Director is immediately informed of the breach.

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.

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 Executive Director's office.

Policy Approved: June 2010