



Policy Title:	Video Surveillance
Policy Type:	Public Service
Policy #:	PS 019-02
Policy Authority:	CEO
Effective Date:	April 2011

PURPOSE

To ensure that, in adopting the use of video surveillance cameras, Clarington Public Library balances the security benefits derived from the use of video surveillance with the privacy rights of individuals, and with adherence to relevant legislation such as the Municipal Freedom of Information and Protection of Privacy Act, the Ontario Human Rights Code, the Canadian Charter of Rights and Freedoms, and the Public Libraries Act.

POLICY

1. Video surveillance is limited to uses that support the safety, security of staff and customers; that safeguard against vandalism, theft, damage and loss of property.
2. Video surveillance will not be used to monitor the inside of areas where the public and employees have a higher expectation of privacy such as the inside of washrooms.
3. Information obtained through monitoring and/or recording will only be released through the authority of the CEO or designate.
4. The Library shall post signs visible to the public at all entrances and/or prominently displayed on the perimeter of the area under video surveillance.
5. The Library's video surveillance system may operate at any time in a twenty-four hour period.
6. Only authorized personnel shall be permitted to operate video surveillance systems.
7. Other than checks to ensure proper equipment functioning, records will be viewed only to investigate a pre-defined occurrence. The information viewed will remain the property of the Clarington Public Library and will be treated as confidential and securely stored.
8. The normal retention period for records is thirty (30) days, followed by destruction by recording over, unless required for evidence. Records required for evidence will be destroyed when no longer required for evidence.

PROCEDURES

General

1. THE CEO or designate shall be responsible for the library's privacy obligations under the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).
2. Any breach of this policy will be investigated by the CEO or designate in order to take appropriate action and/or remedy the breach.
3. Any complaints regarding the video surveillance system should be directed to the CEO. Complaints will be investigated by the CEO or designate.

Signage

Posted signs should include the legal authority for the collection of personal information, the principle purpose 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.

Records

1. All formal requests for video records should be directed to the CEO or designate.
2. MFIPPA provides individuals with a right to access data held about them including those obtained through video surveillance. Severing the personal information in a recording (through technological blurring or blocking) may be necessary to allow individual access.
3. If access to a video surveillance record is required for the purpose of a law enforcement investigation, the requesting officer must complete the Access to Information Request Form and forward it to the library's CEO or designate. The CEO 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 CEO or designate will record the following information the facility's video logbook:
 - a. The date and time of the original, recorded incident including the designated name / number of the applicable camera/ and VCR; the name of the authorized personnel at the time of the incident, the time and date that the copy of the original record was sealed, the time and date the sealed record was provided to the requesting office; whether the record was returned or destroyed after use by the law enforcement agency.
4. Logs will be kept by Administration of all instances of access, to, and use, of recorded data, to enable a proper audit trail. Any video records deemed significant will be copied, stored and labeled with the date, time, and area that was recorded.
5. These records will be retained for a period on one year, after which they will be destroyed unless required for evidentiary purposes by law enforcement officials. The recordings will be completely erased before they are disposed of and a disposal report shall be completed.
6. 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.

7. Viewing will be conducted by at least two (2) persons, one of whom must be the CEO or a designate. If the incident is deemed to be police-reportable, appropriate action will be taken.