Owen Sound & North Grey Union Public Library Policy	Policy # L 24
SUBJECT: Video Surveillance Program	**Date: November 23, 2006 Revised: February 15, 2024 Next Review Date: February 2028**
BOARD AUTHORITY OR STAFF APPROVED: Library Board Resolution: 100-06 Library Board Resolution: 10-24	**Page # 1 of 11**

VIDEO SURVEILLANCE PROGRAM

Policy Statement:

1. The Owen Sound & North Grey Union Public Library (the "Library") is responsible for ensuring the safety of individuals and the security of equipment and property within the scope of the services that the Library provides. Video surveillance systems are a useful tool to accomplish the above goals. The Library recognizes that video surveillance systems have a high potential for infringing upon an individual's right to privacy and that, although video surveillance systems may be required for legitimate operational purposes, their use must be undertaken in accordance with the provisions of the *Municipal Freedom of Information and Protection of Privacy Act* ("MFIPPA") and aligned with the Information and Privacy Commissioner ("IPC") Guidelines for the Use of Video Surveillance.

Purpose:

2. The purpose of this policy is to establish parameters for a video surveillance program that recognizes an individual's right to privacy and that aims to: enhance the safety and security of employees, the public and corporate assets; prevent unauthorized activities on or involving Library property; and reduce risk and liability exposures for the Library.

Scope:

3. This policy applies to:

    a. all Owen Sound & North Grey Union Public Library officers, employees and agents, including full-time, part-time, casual, contract, intern, co-op placement and volunteer individuals;

b. Contractors and service providers and their employees who may work with or operate video surveillance equipment for the Library; and

c. All video surveillance equipment in the care and control of the Library that is located in or at Library properties and facilities.

4. This policy does not apply to:

a. Video or audio recordings of board or committee meetings; or

b. Covert surveillance used as an investigation tool for law enforcement purposes or in contemplation of litigation.

Definitions:

5. For the purposes of this policy,

"Authorized User(s)" means Library employees who have been approved by the CEO / Chief Librarian, or their designate, in consultation with the Manager of Technical Services, or their designates, to operate video surveillance equipment and who have received training consistent with the requirements of this policy;

"Library" means The Owen Sound & North Grey Union Public Library;

"Consistent purpose" means use of personal information in manner that the individual to whom the information relates might reasonably have expected in the circumstances;

"Freedom of Information process" means a formal request for access to records made under MFIPPA;

"Incident" means events or allegations of inappropriate behaviour which would be in violation of law or of a by-law, policy or procedure relating to employee or public conduct;

"Personal information" means recorded information about an identifiable individual, which includes but is not limited to, information relating to an individual's race, colour, national or ethnic origin, sex and age. If video surveillance information displays these characteristics of an identifiable individual or the activities in which he or she engages, its contents shall be considered "personal information" in accordance with MFIPPA;

"Privacy breach" means an incident involving unauthorized disclosure of personal information, including it being stolen, lost or accessed by unauthorized persons;

"Record" means information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a videotape, a machine-readable

record, and any record that is capable of being produced from a machine-readable record;

"Video surveillance equipment" means a video, physical or other mechanical electronic or digital surveillance system or device that enables continuous or periodic video recording, observing or monitoring of personal information about individuals;

"Video surveillance record" means a record of video surveillance information created from the Library's video surveillance equipment.

Policy:

Video Surveillance Equipment

6. Video surveillance equipment will only be installed based on: verifiable reports of incidents of crime; significant safety concerns; or for crime prevention.

7. Video surveillance equipment will only be installed in identified areas where video surveillance is a necessary and viable detection or deterrence tool.

8. Video surveillance equipment will not be installed in or capture recordings of areas where the public and employees have a reasonable expectation of privacy, such as washrooms or change rooms.

9. Video surveillance equipment will be used passively for surveillance purposes (meaning the equipment will not be panned or zoomed remotely) to prohibit the viewing of locations not intended to be monitored.

Responsibility

10. The Chief Librarian and members of Management Team will:

    a. provide oversight and compliance with the policy by all Library employees;

    b. communicate this policy broadly to all employees in their departments;

    c. ensure internal requests for records are necessary for the performance of the requester's duties in the discharge of their functions; and

    d. delegate and assign responsibility regarding who will act on their behalf in following procedures related to this policy in their absence.

11. The Administrative and Facilities Manager, or their designate, will:

a. determine and document the reason for implementation of video surveillance equipment;

b. determine and document the location of video surveillance equipment, description of the viewing area and times when video surveillance will be in effect;

c. determine suitable location(s) for mandatory public notice signage that will provide reasonable and adequate warning that video surveillance is or may be in operation in a particular location;

12. The Technical Services Manager, or their designate, will:

a. assess equipment and system requirements and make necessary arrangements for purchase and installation;

b. inspect video surveillance equipment on a standard schedule and maintain an inspection log;

c. determine and document the corporate video surveillance inventory; and

d. undertake the decommissioning/destruction of video surveillance equipment in a manner that ensures personal information collected by the equipment cannot be retrieved or reconstructed except as authorized by this policy.

13. The Administrative and Facilities Manager, or their designate, in conjunction with the Technical Services Manager, or their designate, will:

a. determine and document the Authorized User(s) for particular video surveillance equipment and ensure they are trained on its use and their responsibilities under this policy; and

b. take all reasonable precautions to ensure that video surveillance equipment is secure and that unauthorized individuals are prohibited from reviewing or accessing information.

14. The Library CEO / Chief Librarian, or their designate, will:

a. ensure the reasons for proposed video surveillance equipment are consistent with the IPC Guidelines for the Use of Video Surveillance;

b. identify potential privacy risks;

c. assist staff to identify appropriate locations for video surveillance equipment and signage;

d. conduct audits, as required, to ensure access to video surveillance information complies with this policy and MFIPPA;

e. respond to all requests for information obtained through video surveillance equipment, and where appropriate, create video surveillance records;

f. ensure compliance with retention periods applicable to video surveillance records;

g. notify the IPC in the event of a privacy breach, where appropriate; and

h. respond to appeals and privacy complaints received through the IPC.

15. Employees will:

a. Refer any external requests for access to or copies of video surveillance information to the Administrative and Facilities Manager or their designate;

b. Refer any internal requests for access to or copies of video surveillance information to Administrative and Facilities Manager for authorization;

c. Report to their manager or supervisor any suspected privacy breaches; and

d. Report to their manager or supervisor any problems with video surveillance equipment.

Notice

16. Signs providing notice of video surveillance shall be posted at public access points for all areas under video surveillance.

17. Video surveillance signage shall clearly indicate that video surveillance is taking place and shall provide information in accordance with s. 29(2) of MFIPPA about:

a. the legal authority for the program;

b. the principal purpose of the program; and

c. contact details for further information.

Access to Video Surveillance Information

18. All persons who have access to information collected from the Library's video surveillance equipment in the execution of their duties for the Library shall sign an undertaking of confidentiality and compliance with this policy (Appendix A).

19. The information collected through video surveillance shall be used only for the purposes of:

a. investigations of incidents involving the safety or security of people, facilities or assets;

b. providing evidence as required to protect the Library's legal rights;

c. responding to a request for information under MFIPPA;

d. investigating an incident or allegation of employee misconduct;

e. investigating an incident involving an insurance claim; or

f. a consistent purpose.

20. The right to create or view video surveillance records is strictly limited and must be undertaken as follows:

a. Public requests: Records related to public requests for disclosure shall be created by the Administrative and Facilities Manager, or their designate, upon a written request made through the freedom of information (MFIPPA) process. Access to these records 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.

b. Internal requests:

i. Records related to investigations involving the safety or security of people, facilities or assets, shall be created by the Administrative and Facilities Manager, or their designate, upon authorization by CEO/ Chief Librarian.

ii. Records related to employee misconduct investigations shall be created by the Administrative and Facilities Manager, or their designate, upon authorization by the CEO / Chief Librarian.

c. Law enforcement requests - Records related to a law enforcement investigation shall be created by the Administrative and Facilities Manager, or their designate, in accordance with s. 32(g) of MFIPPA, when there are reasonable grounds to believe that an unlawful activity has occurred and been captured by video surveillance equipment. These requests shall be made in writing using the "Release of record to law enforcement agency" form attached as Appendix B to this policy.

21. Requests for video surveillance records and release of video surveillance records shall be recorded in the Video Surveillance Request Log by the Administrative and Facilities Manager, or their designate, which log shall include the following:

a. date of request;

b. identity of the requester (who is authorizing the request) and of the recipient (who is being authorized to view the record);

c. date, time, description of event including camera location;

d. reason for the request;

e. method of access (view record/receive copy);

f. date the record was viewed/received.

22. Where a police investigation, related to an emergency situation is underway – meaning there is a genuine, immediate risk to health, life or property – access to video surveillance by law enforcement may be expedited by Authorized Users in accordance with the standard operating procedure (SOP) that is in effect at the time of the occurrence.

23. Live viewing shall be restricted to situations where there is a demonstrably higher likelihood of safety and security concerns involving employees, the public or corporate assets, or the commission of unauthorized activity in the area under surveillance.

24. Live viewing monitors shall be located in areas not accessible by the public and turned off when not in use. If the monitor screen is able to be seen by members of the public, privacy screens will be used.

25. Sound/audio shall only be included in video surveillance records where it is pertinent to the purpose for creating the record.

Records Retention

26. Video surveillance information that is not subject of an authorized request for access shall be considered transitory and shall be automatically erased by the system every twenty-one (21) days in accordance with the Library's records retention schedule.

27. A video surveillance record is subject to retention in accordance with the Library's records retention schedule.

Breach of policy

28. Employees may be subject to criminal charges, civil liability and/or discipline, including but not limited to termination, for a breach of this policy, or provisions of MFIPPA or other relevant statutes.

Policy review

29. This policy shall be reviewed collectively by the CEO / Chief Librarian, or their designate; the Administrative and Facilities Manager, or their designate; and the Technical Services Manager, or their designate:

a. once annually to ensure the effectiveness and compliance with legislation and current business processes; or

b. as required based on legislative changes.

30. The Administrative and Facilities Manager is authorized to make such administrative changes to this policy as appropriate to keep the policy current. Any revision to the intent of the policy shall be presented to Library Board for approval.

31. The forms attached to this policy as appendices may be updated under the direction of the Administrative & Facilities Manager.

Related Policies & Legislation:

32. *Municipal Freedom of Information and Protection of Privacy Act* https://www.ontario.ca/laws/statute/90m56

33. IPC Guidelines for the Use of Video Surveillance https://www.ipc.on.ca/resource/guidelines-for-the-use-of-video-surveillance/

34. L 30 Records Management Policy

35. City of Owen Sound's Video Surveillance Policy CMA66

Appendices:

36. Appendix 'A' - Undertaking of confidentiality and compliance sample

37. Appendix 'B' - Release of record to law enforcement agency sample

Appendix A – Undertaking of confidentiality and compliance with the Library's Video Surveillance Policy.

I (print name) _____, a Owen Sound & North Grey Union Public Library (employee, service provider or authorized consultant) understand that for the purposes of carrying out my duties on behalf of the Library, I may have access from time-to-time to information from the Library's video surveillance equipment in the execution of those duties.
I acknowledge and agree that:

a. All information belongs to the Owen Sound & North Grey Union Public Library.

b. The information shall be under the Library's control and is subject to the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

c. MFIPPA contains provisions that regulate and prohibit the disclosure of personal information. All video surveillance recordings ("information") will be considered personal, as defined in and protected by MFIPPA. The disclosure of any information (personal or otherwise) shall be only in accordance with this Undertaking and the Library's Video Surveillance Policy (the "Policy"), as amended from time to time.

d. I have reviewed and agree to comply with all aspects of the Policy.

e. All information is confidential and I will not access, copy, disclose or provide to any person, or otherwise deal with or use any information, including without limitation any details relating to information (whether personal or otherwise), except as specifically authorized by the Library and in accordance with the Policy.

f. I will not use or refer to any information for any purpose other than as specifically authorized by the Library as set out in the Policy.

g. I will store any information that I have access to in a manner as directed by the Library and in accordance with the Policy.

h. I will not destroy or remove any information from the Library's premises except as specifically authorized by the Library or in accordance with the Policy.

i. I will not leave any information unsecured and I will take all measures reasonably necessary to ensure that persons not authorized to view or access the information are not in any manner provided with such opportunities.

j. I will report any unauthorized access, copying, disclosure or other dealing or use of the information, of which I become aware, immediately to my supervisor, and will cooperate fully with the Library, the Office of the Information and Privacy Commissioner or any other investigative body in the investigation of same.

I acknowledge that failure to comply with this Undertaking or with the Policy and any related procedures may result in disciplinary action being taken or termination of my contract, as may be applicable, as well as civil or criminal liability.

Name:		Job Title/Company:	
Signature:		Date:	

Appendix B - Release of record to law enforcement agency

The following information is being requested under section 32(g) of the *Municipal Freedom of Information and Privacy Act* which allows for disclosure of records containing personal information for the purposes of aiding a law enforcement investigation.

<table>
<tr><th colspan="3">Attending Law Enforcement Officer to complete this section:</th></tr>
<tr><td colspan="3">Date of occurrence:</td></tr>
<tr><td colspan="3">Time of occurrence:</td></tr>
<tr><td colspan="3">Location of occurrence:</td></tr>
<tr><td colspan="3">Description of occurrence (i.e., MVA):</td></tr>
<tr><td colspan="3">Your Investigation Number:</td></tr>
<tr><td colspan="2">Review Original Record: ☐ yes ☐ no</td><td>Copy requested: ☐ yes ☐ no</td></tr>
<tr><td colspan="3">I _____ (Officer Name) request the above video footage, which may contain personal information, to aid an investigation undertaken by _____ (Law Enforcement Institution) with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.</td></tr>
<tr><td>_____
Signature of Investigating Officer</td><td>_____
Badge Identification Number</td><td>_____
Date (yyyy-mm-dd)</td></tr>
</table>