POLICY

Policy Type: **Facility Policy** **Policy Number:** **06-06**
Policy Title: **Security Video Surveillance Policy**

1.0 Policy Statement

The St. Thomas Public Library Board acknowledges the need to balance the responsibility to promote a safe and secure environment and to protect the privacy of individuals.

The St. Thomas Public Library Board supports the use of security video surveillance as one tool in its overall safety and security strategy.

2.0 Purpose and Scope

This Policy is intended to govern the use of security video surveillance at St. Thomas Public Library in accordance with privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

This Policy applies to camera surveillance systems, surveillance monitors and camera recording devices at St. Thomas Public Library that are used for security purposes.

3.0 Definitions

Authorized Personnel: St. Thomas Public Library employees, City of St. Thomas employees, contractors and agents whose duties require them to operate security video surveillance equipment and/or access security video surveillance information and records.

Security Video Surveillance: A security video surveillance system in which video signals are transmitted from one or more cameras by a cable to restricted digital video recorders.

Security Video Surveillance Equipment: Any physical, mechanical, electronic, digital or wireless device or apparatus such as cameras, monitors and recording devices used to observe and/or record actions or events in a certain area.

Design: To plan for the installation of security video surveillance equipment; includes equipment, camera location(s) and positioning.

Facilities: Properties that are leased or owned by the St. Thomas Public Library Board.

Personal Information: Defined by MFIPPA as 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 a video system displays these characteristics of an identifiable individual or the activities in which the individual is engaged, its contents will be considered "personal information" under MFIPPA.

Record: A record is created any time information collected through security video surveillance has been preserved, including: security video surveillance recordings or images that have been saved to a computer, a computer disk (CD), a USB flash drive or any other device used to store or transfer information or images captured by security video surveillance equipment.

4.0 Administration

4.1 Use of Security Video Surveillance System

Security video surveillance equipment is any physical, mechanical, electronic, digital or wireless device or apparatus such as cameras, monitors and recording devices used to observe and/or record actions or events in a certain area.

The use and installation of any St. Thomas Public Library security video surveillance system consists of the process described below.

4.2 Purposes of Collection and Use of Information

St. Thomas Public Library uses security video surveillance in its overall strategy for the safety and security of Library employees, clients, residents, visitors, and property. Security video surveillance, when properly deployed, is effective in ensuring a safe and secure environment at the Library.
Post-event, the Library may use security video surveillance recordings to assist with the investigation and resolution of the full spectrum of facility related incidents, claims and complaints, including employee misconduct and to assist with responding to requests from law enforcement agencies that are for evidentiary or investigative purposes.

4.3 Design and Installation

The Library CEO, or designate shall prior to the installation of any security video surveillance equipment complete a Privacy Impact Assessment, which would identify and mitigate potential privacy risks, including a determination of the camera's field of view and confirmation that security countermeasures/tools other than the use of cameras have been considered and determined to be impractical.

4.4 Field of View

The field of view captured by cameras will be determined on the basis of reasonable and justifiable grounds for the provision of safety and security. Security video surveillance equipment shall not be positioned in a manner that allows viewing into areas where individuals generally have a higher expectation of privacy, such as washrooms, change rooms, and private buildings. Furthermore, video monitors shall not be located in an area that enables viewing by the general public.

Any alteration of a camera's field of view must be approved by the Library CEO, or designate.

4.5 Securing Video Recording Equipment

Video recording equipment shall be secured to prevent unauthorized access.

4.6 Hours of Operation

Security video surveillance may be in operation at any time. While security video surveillance cameras are continuously recording, they may only be periodically monitored by Authorized Personnel.

5.0 Notice of Collection of Personal Information

Notification to the public of the use of security video surveillance shall be provided by ensuring that:

1. Signs are posted at all entrances to areas under security video surveillance to provide the public with reasonable notice that security video surveillance is or may be in operation. Refer to Appendix A: Sample security video surveillance sign.

2. The following written notice is posted on the St. Thomas Public Library website:

Notification - St. Thomas Public Library Security Video Surveillance

The use of a security video surveillance system is undertaken in accordance with the St. Thomas Public Library Security Video Surveillance Policy. Personal information is collected for security purposes in and around facilities that are owned or leased by St. Thomas Public Library to ensure the safety and security of employees, clients, users and visitors. Security video surveillance cameras are continuously recording but may only be periodically monitored by Authorized Personnel.

Further information concerning the use of security video surveillance is available in the St. Thomas Public Library Security Video Surveillance Policy and by contacting the Library CEO, or designate at 519-631-6050, 153 Curtis Street, St. Thomas, Ontario, N5P 3Z7.

6.1 Retention and Disposal of Security Video Surveillance Recordings and Records

6.2 Security Video Surveillance Recordings

Security video surveillance recordings shall be retained for 72 hours from the time of collection. The recordings will automatically be overwritten (erased) after the 72 hour period. St. Thomas Public Library shall not retain security video surveillance recordings beyond 72 hours except in circumstances where the Library has created a record in accordance with this Policy, including in response to a request for disclosure or retention.

6.3 Security Video Surveillance Records

Security video surveillance records shall only be created in respect to security and safety incidents, or in response to a request for preservation or disclosure. Records shall be retained for one year, as per MFIPPA guidelines.

6.3 Access to Video Records and Equipment

Access to security video surveillance records shall be restricted to authorized personnel for purposes that are consistent with this policy.

6.4 Control and Responsibility of Records

All St. Thomas Public Library employees, contractors, and agents acknowledge that all records created or used by the security video surveillance system are under the control of the Library and are subject to the provisions of applicable legislation.

6.5 Viewing Live Video

Access to live video from security video surveillance cameras for operational purposes is restricted to authorized personnel.

7.0 Disclosure of Images or Recordings

St. Thomas Public Library shall not disclose security video surveillance images or recordings to any individual or organization except:

- to authorized personnel for purposes that are consistent with the purposes for collection and use of security video surveillance images or recordings such as in respect of security and safety incidents or in respect of facility related incidents, claims and complaints.
- to a law enforcement agency in Canada as requested for evidentiary or investigative purposes. The records may be released upon submission of a Disclosure of Personal Information to a Law Enforcement Officer form.
- by the Library’s designated Freedom of Information and Privacy Coordinator in accordance with the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).
- As otherwise permitted or required by the application of MFIPPA or other legislation.

7.1 Log

All instances where security video surveillance recordings are created as a record and disclosed in accordance with this policy shall be documented by noting the date and time the records were created, the name of the authorized personnel who created the record, and the authorized personnel or agency to whom the record was disclosed.

The log shall remain in a secure location and shall be restricted to personnel, as authorized by the Library CEO, or designate.

8.0 Unauthorized Access and/or Disclosure (Privacy Breach)

A Library employee, contractor or agent who becomes aware of any unauthorized access, disclosure, use, copying, modification or destruction of any record that contains personal information shall immediately notify the Library CEO, or designate.
The Library CEO or designate shall investigate any instances of unauthorized access or disclosure of personal information and mitigate the extent of the privacy breach with assistance from the Library's designated Freedom of Information and Privacy Coordinator in accordance with the Privacy Breach Protocol.

9.0 Responsibilities

Library CEO, or designate is responsible for:

• The procurement, installation, use and/or operation of security video surveillance equipment at facilities owned and operated by St. Thomas Public Library;

• Developing specific procedures and practices for the administration of security video surveillance to ensure compliance with the requirements set out in this Policy;

• Ensuring that the design and installation of all security video surveillance equipment meets the requirements set out in this Policy;

• Ensuring that security video surveillance equipment is functioning properly at all times;

• Ensuring that recorded security video surveillance footage is only accessed and used for its originally intended purpose;

• Ensuring that all authorized personnel have received training and completed the Security Video Surveillance Policy Training Checklist;

• Performing annual reviews of all security video surveillance systems to determine whether their installation and continued use is still justified in accordance with the requirements under MFIPPA;

• Providing information to the Library's designated Freedom of Information and Privacy Coordinator, as requested;

• Ensuring that information is available to law enforcement agencies, as required;

• Investigating any instances of unauthorized access or disclosure of personal information and mitigating the extent of the privacy breach with assistance from the Library's designated Freedom of Information and Privacy Coordinator;

• Ensuring compliance with this Policy; and

• Reviewing this Policy every three (3) years after it is adopted.

Authorized Personnel whose duties require them to operate security video surveillance equipment or to access security video surveillance information and records are responsible for:

• Ensuring that personal information is only accessed for the purposes set out in this Policy;

• Ensuring that the appropriate documentation is completed any time security video surveillance information is accessed or disclosed;

• Responding to law enforcement agency requests;

• Signing of Authorized User Confidentiality Agreement; and,

• Ensuring compliance with this Policy.

10.0 Monitoring/Contraventions

This Policy shall be monitored by the Library CEO or designate.

The Library CEO or designate shall investigate and address any possible or founded contraventions of this Policy and related legislation. Failure to comply with this Policy may result in disciplinary action, up to and including termination of employment or contract by St. Thomas Public Library.

Approved Date: September 9th, 2020
Supercedes Date: none
Review Date: September 2023 (every 3 years)
Reference: Board Meeting September 9th, 2020

Appendix A
Sample Security Video Surveillance Sign

ATTENTION

Video Surveillance Cameras are in use on this Property.

The collection of personal information is authorized under the Security Video Surveillance Policy #06-06. More information available at

stthomaspubliclibrary.ca/cameras

Appendix B
Disclosure of Personal Information to Law Enforcement Officer Form

Disclosure Information (Print information)

Name of Law Enforcement Officer	
Badge Number	
Agency	
Description of Record Being Sought	
Police Report #	
Date Record Sought	

By signing below, the representative of the law enforcement agency certifies that the record(s) sought are required by the named law enforcement agency to aid in an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

After Use Record Shall Be (Please check appropriate)

Destroyed: ☐ Returned: ☐

Disclosure Record (name and signature)

Date: _____ _____

Authorized Personnel

Name: _____

Date: _____ _____

Signature, Law Enforcement Officer

Name: _____

Appendix C

Log

Location of Security Video Surveillance Camera(s):_____

Authorized Onsite Personnel_____

_____

Date and time Record Created	Name of staff who created record	Reason for access: (eg. Disclosure to Law Enforcement Officer Form, MFIPPA Request)	Date and time of video footage:	Authorized by:

APPENDIX D Privacy Breach Protocol

A privacy breach occurs when there is unauthorized access, collection, use, disclosure, copying, modification, or destruction of personal information, contrary to the privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act.

When faced with a privacy breach, the following actions must be undertaken immediately:

NOTIFICATION

Notify the Library CEO or designate.

INVESTIGATION OF PRIVACY BREACH

The Library CEO or designate shall inform the Freedom of Information and Privacy Coordinator of the privacy breach and together, they will investigate the privacy breach.

A record will be kept of all investigations of privacy breaches in accordance with requirements of the Information and Privacy Commissioner.

CONTAINMENT OF PRIVACY BREACH

The Library CEO or designate and the Freedom of Information and Privacy Coordinator will undertake the following steps in response to the privacy breach.

1. Identify the nature and scope of the privacy breach.

2. Ensure that no copies of the personal information have been made or retained by the individual(s) who was not authorized to receive or use the information.

3. Determine whether the breach would allow unauthorized access to any other personal information and take necessary steps to prevent a further breach.

4. Retrieve and secure any personal information that has been collected, used, copied, modified or disclosed without authority.

5. Determine whether further action is required regarding the individual(s) involved with the privacy breach.

NOTIFICATION TO AFFECTED INDIVIDUAL(S)

1. Notify the affected individual(s) whose personal information was collected, used, copied, modified or disclosed without authority if it is determined that the breach poses a real risk of significant harm, taking into consideration the sensitivity of the information and whether it is likely to be misused. If law enforcement is involved, ensure that notification will not interfere with any investigations.

2. Provide a description and extent of the breach and advise the individual(s) of the steps that have been undertaken to address the breach and how a similar breach would be prevented from happening.

3. Advise individual(s) who they can contact for additional information and assistance from the Library and of their right to complain to the Information and Privacy Coordinator.

REVIEW OF POLICIES, PROCEDURES, AND TRAINING

A review of policies, procedures, and training programs will be undertaken to determine whether any changes are required and that all personnel/contractors are appropriately educated and trained with respect to compliance with the Security Video Surveillance Policy and Procedures and the privacy protection provisions of the Municipal Freedom of Information and Protection of Privacy Act.

Appendix E Privacy Impact Assessment

Facility Name	
Address	
Location of security video surveillance system	--
Date	

1. Please describe the security video surveillance system to be used and how its set-up adheres to the Library's Security Video Surveillance Policy. Attach floor/site plan with camera and equipment locations.

2. Provide justification for the use of a security video surveillance system at this particular facility or property including verifiable, specific reports of incidents of crime or significant safety concerns. e.g. Police Reports, Health and Safety Committee minutes, Departmental Occurrence Reports, Internal memos.

3. Video surveillance should only be considered after other measures of deterrence or detection have been considered and rejected as unworkable. Have the following security measures been considered and rejected as unworkable or less effective?

	Security Measure	**Yes**	**No**	**Comments**
A	Security Procedures e.g. end of day lock up checklist			
B	Panic Alarms			
C	Door Locking Hardware			
D	Alarm System			
E	Access Control System			
F	Signage			
G	Security Guard/Officer Patrols			
H	Lighting			
I	Other - Please Specify			

4. An assessment should be conducted on the effects that the proposed security video surveillance system may have on personal privacy and the ways in which any adverse effects can be mitigated. Have the following effects and mitigation strategies been considered?

	Effects and Mitigations Strategies	**Y**	**N**	**Comments**
A	Is the security video surveillance system proposed to be located in an area that will minimize privacy intrusion?			
B	Is the security video surveillance system proposed to be located in a location where the public and/or employees do not have a higher expectation of privacy? e.g. Not in a change room washroom.			
C	Is the location of the proposed security video surveillance system visible?			

D	Can the security video surveillance be restricted to the recognized problem area?			
E	Is space allocated for proper security video surveillance system in use?			

5. The proposed design and operation of a security video surveillance system should minimize privacy intrusion. Have the following design and operation factors been considered for the proposed facility?

	Measures to mitigate privacy impact	**Yes**	**No**	**Comments**
A	Can the Proposed camera be restricted through hardware or software to ensure that it cannot be adjusted or manipulated to overlook spaces that the PIA has not been completed for?			
B	Is the reception equipment going to be located in a strictly controlled access area?			
C	Can the security video surveillance monitor be installed in such a way that it will be hidden from public view?			
D	Are there other measures in place to mitigate privacy impact?			

6. Please provide the following information related to this initiative.

A. Who will be authorized to access video surveillance equipment (name, staff positions and/or potential vendors)?

B. Where are recordings proposed to be stored? (e.g. network server on site, third party servers, on cloud, within or outside of Ontario or Canada)

C. What security measures will be put in place to protect where the recordings are

stored? (e.g. locked server room, through use of logins/passwords, etc.)

D. Does the system have the ability to be altered to protect the privacy of other individuals (e.g. blurring of faces or licence plates)?

E. Does the system have the ability to audit who accessed it, when and what they did? (e.g. what video they reviewed, did they copy the video?)

F. Will the proposed security video surveillance system be linked to other databases (e.g. FOB/Key access systems, resident databases, etc.)?

7. Prior to installing a security video surveillance system and where feasible to do so, the Library should identify those individuals who reasonably may be affected by the security video surveillance system and consult with them on the system's necessity and impact.

	Stakeholder	**Particular Interest**	**Comment/Concerns**
A	Neighbouring businesses/residents	-	-
B	Patrons	-	-
C	Library Staff		-

D	Police Services	-	

Privacy Impact Recommendations

Indicate recommendations for changes and/or approval.

_____

_____

_____

_____

Library CEO, or designate

Signature_____Date _____

Freedom of Information and Privacy Coordinator

Signature _____ Date _____

APPENDIX F Authorized User Confidentiality Agreement

I, (print name)_____, a St. Thomas Public Library (employee, contractor or agent) 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 security video surveillance system in the execution of those duties, including security video surveillance record(s) and digital video recorder(s) and related equipment.

I acknowledge and agree that:

1. All information belongs to the St. Thomas Public Library.

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

3. 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 Security Video Surveillance Policy.

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

5. 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.

6. 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.

7. I will store any information that I have access to in a manner as directed by the Library and in accordance with the Policy. I further agree not to destroy or remove any information from the Library's premises except as specifically authorized by the Library and in accordance with the Policy. I will not leave any information unsecured and 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.

8. 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, upon request, cooperate fully with the Library, the Freedom of Information and Privacy Coordinator or any other investigative body in the investigation of same.

9. 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 (print)	
Job Title	
Signature	
Company Name/ Department	
Date	

Appendix G Security Video Surveillance Policy Training Checklist

Employee or Authorized Personnel:
Department or Company:
Position Title:

1. Policies and Procedures

		Yes	No
A	Has received a copy of, read and understood the St. Thomas Public Library's Security Video Surveillance Policy?		
B	Has received a copy of, read and understood all appendices to the St. Thomas Public Library Security Video Surveillance Policy?		

2. Roles and Responsibilities

		Yes	No
A	Understands the roles and responsibilities of the designated staff the Library, Security Video Surveillance Operators, and the Freedom of Information and Privacy Coordinator.		
B	Understands and will carry out the duties and responsibilities of the Operator.		

3. Guidelines for the Implementation of a Security Video Surveillance System

		Yes	No
A	Is aware that security video surveillance equipment should only be installed and used to monitor those spaces that have been identified as requiring security video surveillance.		
B	Is aware that no person shall adjust or manipulate cameras to view spaces that are not intended to be covered by the security video surveillance policy.		
C	Is aware that equipment should never be used to monitor the inside of areas where the public and employees have a higher expectation of privacy. (i.e. washrooms, change rooms)		
D	Is aware that all security video surveillance installations must be clearly marked to advise staff and members of the public that security video surveillance is in use.		
E	Is aware that signs shall be posted at all entrances and/or on the perimeter of the grounds under security video surveillance.		

4. Security Video Surveillance Equipment / Records

		Yes	No
A	Understands the need for proper identification and labelling of any records that need to be created.		
B	Is aware that each Security Video Surveillance Authorized Personnel shall maintain a logbook to record all activities related to security video surveillance devices and records and that each entry will detail authorized staff, date, time, and type of access.		
C	Is aware that Security Video Surveillance Authorized Personnel must document all information regarding the use, maintenance, and storage of records in the logbook, including all instances of access to, and use of, recorded material to enable a proper audit trail.		
D	Is aware that Security Video Surveillance Authorized Personnel may not deliberately enter false or incomplete information or delete existing information in any logbook and may not take any unauthorized action that would cause the destruction or alteration of any information contained in any logbook.		
E	Is aware that Security Video Surveillance Authorized Personnel shall not make any changes to the identificationor labels of records either in hardcopy or electronic formats.		
F	Is aware that all tapes or other storage be devices that are not in use must securely stored in a locked receptacle located in an access-controlled area.		
G	Is aware that Security Video Surveillance Authorized Personnel shall not make any copies of data/images in any format from the security video surveillance system except in accordance with the protocols set out in the Security Video Surveillance Policy.		

5. Access to Security Video Surveillance Records

		Yes	No
A	Is aware that Security Video Surveillance Authorized Personnel may access information only when necessary to perform work assigned by the Library CEO or designate to accomplish the Library's mission and objectives.		
B	Is aware that Security Video Surveillance Authorized Personnel must not access or use information from any component(s) of the Security Video Surveillance system files or database for personal reasons.		
C	Is aware that access to the security video surveillance records e.g. storage devices, logbook entries, CD's, videotapes shall be restricted to authorized personnel only.		
D	Is aware that Security Video Surveillance Authorized Personnel shall not disclose any personal information and that disclosure should only occur in accordance with the Security Video Surveillance Policy.		

E	Is aware of and understands the use of the Law Enforcement Officer Request Form.		

6. Viewing Images

		Yes	No
A	Understands that security video surveillance monitors should be concealed as much as possible from the general public and unauthorized personnel.		
B	Understands that any images from the camera must be viewed in a private, controlled area that is not accessible to unauthorized personnel.		

7. Retention and Disposal of Records

		Yes	No
A	Is aware that a Security Video Surveillance Authorized Personnel must not dispose, destroy, or erase any record without proper authorization and in accordance with the Library's Policy.		
B	Is aware that no records shall be made of security video surveillance recordings except in accordance with the Security Video Surveillance Policy.		
C	Understands that security video surveillance records will be retained in accordance with the Library's policy.		
D	Understands that the Security Video Surveillance Authorized Personnel shall take all reasonable efforts to ensure the security of records in the Library's custody and control.		
E	Understands that all storage devices must be disposed of in accordance with an applicable technology asset disposal process ensuring personal information is erased, shredded, or burned and cannot be retrieved or reconstructed.		

8. Unauthorized Access and / or Disclosure

		Yes	No
A	Understands that any Security Video Surveillance Authorized Personnel and/or any Library staff who become aware of any unauthorized disclosure of a video surveillance record in contravention of the St. Thomas Public Library Security Video Surveillance Policy and/or a potential privacy breach are to immediately notify the St. Thomas Public Library CEO or designate.		
B	Understands that intentional wrongful disclosure, or disclosure caused by negligence, by employees of the Library may result in disciplinary action up to and including dismissal and that intentional wrongful		

	disclosure caused by negligence by service providers (contractors) to the Library, may result in termination of their contract.		

9. Inquiries from the Public

		Yes	No
A	Is aware that any Security Video Surveillance Operator receiving an inquiry from the public regarding the Security Video Surveillance Policy shall direct the inquiry to the Library's Freedom of Information and Privacy Coordinator?		

10. Audit

		Yes	No
A	Is aware that the Library CEO, or designate will designate staff to conduct random site visits or audits to ensure the Security Video Surveillance Policy is being followed?		

_____ _____ _____

Authorized Personnel Name Signature Date

_____ _____ _____

Supervisor Name Signature Date