Video Surveillance System Policy
P-CS-23-04

1. Policy

Policy Number:	P-CS-23-04
Policy Name:	Video Surveillance System Policy
Effective Date:	06-2023
Last Revised:	09-2023
Last Reviewed:	09-2023

2. Policy Purpose

The purpose of this Policy is to outline the responsible use of the Video Surveillance System, as it is used for recording, monitoring, and storing video on all properties owned or leased by the Town of Niagara-on-the-Lake for the express purpose of providing safety and security of all persons and property, including preventing and deterring crime, identifying suspects, and gathering evidence.

3. Scope

This procedure applies to all employees whose duties include requesting, installing, accessing and monitoring video security equipment and video footage of Town of Niagara-on-the-Lake facilities and properties but shall not apply to videotaping or audio taping of Council and Committee meetings, communications productions, court proceedings, or any covert security that may be used for law enforcement purposes.

4. Definitions

TERM	DEFINITION
Act	means the *Municipal Freedom of Information and Protection of Privacy Act* or the *Personal Health Information and Protection Act.*
Consistent Purpose	means the individual to whom the information relates might have reasonable expectations regarding the use and disclosure of their personal information.
Control (of a record)	means the power or authority to make a decision about the use of disclosure of a record.
Custody (of a record)	means the keeping, care, watch, preservation or security of a record for a legitimate business purpose. While physical possession of a record may not always constitute custody, it is the best evidence of custody.
Destruction	means the physical disposal of records by means of shredding, disintegrating or recycling including the electronic disposal of data by means of deletion and overwriting. This also includes the destruction of data residing on computers

	and electronic devices supplied or paid for by the Corporation.
Head	the individual(s) that is designated by the Town to act as the "head" for the purposes of the Municipal Freedom of Information and Protection of Privacy Act.
Information and Privacy Commissioner (IPC)	meant the Information and Privacy Commissioner of Ontario, commonly referred to as the IPC. The IPC hears appeals of decisions made by the "head" of an institution, issues binding orders, conducts privacy investigations, and has certain powers relating to the protection of personal privacy.
Municipal Freedom of Information and Protection Privacy Act	means the legislation that governs access to and the privacy of the Town's records containing personal information.
Personal Information	means recorded information about an identifiable individual including: • Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation; • Information relating to the education, medical, psychiatric, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; • Any identifying number, symbol or other particular assigned to the individual; • The personal opinions or views of the individual except if they relate to another individual; • Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence; • The views of opinions of another individual about the individual; and • The individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual. Privacy Breach – means an incident involving unauthorized disclosure of personal information, including it being lost, stolen or accessed by unauthorized persons.
Privacy by Design (PbD)	means the privacy standard developed by the Information and Privacy Commissioner (IPC) of Ontario that the Town will utilize to build privacy and data protection, into the design specification and architecture of information and communications systems and technologies at the beginning, in order to facilitate compliance with privacy and data protection principles.

Record(s)	means any record of information, however recorded, whether in printed form, on file, by electronic means or otherwise and includes: • Correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics and any copy thereof, and • Subject to regulations, any record that is capable of being produced from a machine-readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution. Retention Period – means the period of time during which a specific record or record series must be kept before records in that series may be disposed of.
Retention Schedule	means a list of all the record classifications and their corresponding retention periods. The schedule also identified which records are deemed vital, which are archived and who is the responsible department or official record holder.

5. Policy Statement

This policy defines the criteria and process associated with the installation and use of video security equipment to ensure that it is used only to promote the safety and security of the Town of Niagara-on-the-Lake, the public, employees, assets, and property in accordance with the provisions of relevant legislation and established policies and procedures.

6. Policy Details

This policy addresses requirements and responsibilities with respect to:

- The installation of Video Surveillance Systems
- The operation of Video Surveillance Systems
- The use of information obtained through Video Surveillance Systems,
- Custody, control, access to and retention of Records created through Video Surveillance Systems

7. Procedures

Please see Appendix A.

8. Forms/Appendices

- Appendix A: Video Surveillance Procedures
- Appendix B: Notice to the Public
- Appendix C: Instant Access Form
- Appendix D: Video Request Form
- Appendix E: Public Notices
- Appendix F: Location of Video Security

9. Responsibilities

POSITION or OFFICE	RESPONSIBILITIES
Director of Corporate Services	1. Responsible for the overall video security program. This is further delegated to the Manager of Information Technology to operate and maintain the video security systems.
Manager of Information Technology	1. Responsible for the life cycle management of the authorized video security systems, including the specifications, equipment standards, installation, maintenance, replacement and disposal. They are also responsible for the technical aspects of the video security systems. 2. Responsible for the day-to-day operation of the system in accordance with this policy.
Town Clerk	1. Responsible for following this procedure along with the coordination and performance of audits. The Town Clerk is also responsible for the Town's responsibilities under the applicable Acts, including but not limited to the, the Municipal Freedom of Information and Privacy Protection Act.

10. Related Information

N/A

11. Contacts

Please direct any questions regarding this policy to:

OFFICE	PHONE	EMAIL

Director of Corporate Services	905-468-3266	Kyle.freeborn@notl.com

POLICY GOVERNANCE	
Policy Number:	P-CS-23-04
Effective Date:	2023-06-26
Last Reviewed Date:	2023-09-26
Target Review Date:	2025-09-26
Approval Authority:	
Policy Owner:	Director of Corporate Services/Treasurer
Responsible Office:	Corporate Services
Supplemental Documents:	

Appendix A: Procedure

1.1. Planning Criteria for Video Security Systems

To ensure the safety of staff and the public, as well as, a deterrent and detection mechanism against vandalism to buildings and properties, video security cameras may be used in accordance with the following criteria:

a) To assist in the security of staff and the public by providing a record of an incident, or acting as evidence for prosecution;
b) To deter and/or assist in the identification of individuals that may put staff and public at risk at Town facilities and properties;
c) To respect the principles of the *Municipal Freedom of Information and Protection of Privacy Act*, and the *Municipal Act*;
d) To provide security without limiting general public activities;
e) To be installed without notice as part of a specific investigation where criminal activity is suspected or known.

The Town will endeavour to ensure the proposed design and operation of the video security system minimizes privacy intrusion to that which is absolutely necessary to achieve its required, lawful goals.

Any agreements between the Town and service providers must stipulate all video security programs are under the Town's custody and control.

A service provider who is considered to be in breach of the policy and procedure and the applicable acts may lead to penalties and up to the termination of the contract. In addition, full legal action and an investigation may be required, depending on the nature of the breach of this policy.

2. The Design, Installation and Operation of Video Security equipment

2.1. The Town shall maintain control of, and responsibility for, the video surveillance system at all times.
2.2. Viewing equipment such as video cameras should only be installed in identified public areas where video security is a deemed necessity and viable detection or deterrence activity. Appropriate areas for video security include entrances, exits, general-purpose areas, corridors, receiving areas, parking lots, and exterior building perimeter. The equipment will operate up to 24 hours/seven days a week and/or within the limitation of the system, for example, digital storage, power disruptions and serviceability/maintenance.
2.3. The equipment will be installed in such a way that it only monitors those spaces that have been identified as requiring video security. Cameras should not be directed to look through the windows of adjacent properties, or be aimed at areas where people have a heightened expectation of privacy.

2.4. If cameras are adjustable by operators, this should be restricted, if possible, so operators cannot adjust or manipulate them to overlook spaces that are not intended to be covered by the video security program.
2.5. No work on the systems will be allowed without an authorized staff present for the duration of the work.
2.6. Equipment will not monitor the inside of areas where staff and the public have a higher expectation of privacy, such as in change rooms or washrooms.
2.7. Viewing equipment should be kept in a strictly controlled access area. Only controlling personnel, or those authorized should have access to the controlled access area and reception equipment.
2.8. Video monitors should not be in a position that enables public viewing of the images that are being reviewed for the purpose of disclosure.
2.9. Video recorded material shall be stored in a controlled-access location outside of public view. Only designated personnel will have access to this location and to video recorded material.
2.10. Periodic maintenance of video security equipment shall be the responsibility of the Town's Information and Technology Division according to a schedule that will ensure efficient operation of the system.

3. Confidentiality:

3.1. Access to the personal information collected under a video security system on a given site is only afforded to Town authorized employees and contracted service providers with specific duties pertaining to the supervision, operation and maintenance of the system and for the proper, secure storage and destruction of video recordings regardless of the software medium used to store images.
3.2. All video footage that is uploaded from the video security software will be placed on an encrypted digital source for storing personal information captured by video security.
3.3. Any agreements between the Town and service providers shall state that the records dealt with or created while delivering a video security program are under the Town's control and are subject to the *Municipal Freedom of Information and Protection of Privacy Act.*
3.3.1. Town employees and contracted service providers will comply with the requirements of this policy and the *Municipal Freedom of Information and Protection of Privacy Act* in performing any duties related to a Town-approved video security system.
3.3.2. Town employees and contracted service providers will be subject to discipline, up to and including termination of employment or service to the site, for knowingly or deliberately breaching this policy or the provisions of the

Municipal Freedom of Information and Protection of Privacy Act or other relevant statutes.

3.3.3. Where a service provider fails to comply with this policy or the provisions of the *Municipal Freedom of Information and Protection of Privacy Act*, such a failure will be considered to be a breach of contract leading to penalties that include but are not limited to contract termination.

3.4. Town employees and the employees of service providers performing any duties related to the operation of a Town approved video security program are required to sign an undertaking of confidentiality.

4. NOTICE:

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

4.1.1. The Town shall post signs, visible to staff and members of the public, at all entrances and/or prominently displayed on the perimeter of the grounds under security.

4.1.2. 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, the title, business address, and telephone number of someone who can answer questions about the collection, see Appendix “D”

4.1.3. The Town will provide notice to the public on the Town’s website as well as a link on each of the Department's websites. The notice shall be clear, and language-neutral along with a graphic depiction of the use of video security.

FORMAL ACCESS REQUEST PROCESS

4.2. All requests for video records should be directed to the Office of the Town Clerk.

4.3. A person requesting access to a records should request in writing either through the online form or by submitting a printed form. The individual requesting the information must:

4.3.1. Provide sufficient detail, such as the approximate time and date, the location, (if known) of the incident, to enable an experienced employee of the Town, upon reasonable effort, to identify the record; and,

4.3.2. At the time of making the request, pay the prescribed fees as provided for under the *Municipal Freedom of Information and Protection of Privacy Act.*

4.3.3. The Town may levy additional fees to prepare and redact, as per the *Municipal Freedom of Information and Protection of Privacy Act*, any information that is outside of the scope of the request.

4.4. If the Town has the ability to redact or remove personal information of individuals that may have been captured on the video security and would be considered exempted information by using tools and techniques such as:

- Digitizing analogue footage to enable the use of more powerful editing tools.
- Blacking out or blurring images of individuals that are not subject to the request, however,

- If the Town does not have the ability to redact or remove personal information, they shall outsource this requirement, and forward the cost to the individual(s) requesting the information.

6. ACCESS: LAW ENFORCEMENT

6.1. If access to a video security record is required for the purpose of a law enforcement investigation, the requesting Officer must complete a Law Enforcement Request Form, Appendix "C", and forward the form to the Office of the Town Clerk. The Clerk's department will provide the recording for the specified date and time of the incident.

6.2. The Clerk's department will record the following information as per the guidelines from the Information Privacy Commissioner outlined in the MFIPPA manual:

6.2.1. The date and time of the original, recorded incident including the designated name/number of the applicable camera and DVR. For example main hallway, camera 1;

6.2.2. The time and date the record was copied and provided to the requesting Officer;

6.2.3. The name and title of the individual who made the copy for the requesting Officer;

6.2.4. If the record will be returned or destroyed after use by the Law Enforcement Agency.

7. VIEWING IMAGES

7.1. When recorded images from the cameras must be viewed by law enforcement or for investigative reasons, this must only be completed by an individual(s) authorized by the Town in a private, controlled area that is not accessible to other staff and/or visitors.

8. RETENTION, SECURE STORAGE, ACCESS TO, AND DISPOSAL OF VIDEO RECORDS:

8.1. Video recorded material on a portable device, that is encrypted, which may contain elements of proof shall be stored in a locked, secure location to ensure the integrity of information, and to be available should law enforcement request them. Access to recorded material shall be limited to the Office of the IT Manager, and Director of Corporate Services and the Town Clerk.

8.2. Access to the video recording equipment should be limited to the Manager of Information Technology, or their approved delegate. Appendix "B", Part A – Video information of the instance of Access Form should be completed when access to the video recording equipment is requested for a copy of a video image.

8.3. Recorded data on the recording equipment shall be maintained for a maximum of thirty (30) days or less dependent on allowable digital video storage.

8.4. A portable device on which video recorded material is stored and encrypted (including a computer drive, CD ROM, USB drive, or any other device used to store video recorded material) must be labeled and securely stored and, in accordance with the Records Retention Bylaw, be securely disposed of in such a way that the personal information cannot be reconstructed or retrieved. Appendix "B", Part B – Destruction of Video Recorded Data of the Instance of Access Form must be completed.

8.5. If video recorded material on a portable device is required as part of an ongoing investigation, it shall be retained for a least one year and in accordance with the records retention schedule.

8.6. The Clerk's department, shall approve the release of records when law enforcement requests to view, or to take a copy of, video images. In all cases when video images are released as part of a police investigation (see video release form to law enforcement) must be completed.

8.7. Any staff member or member of the public who has been recorded by video security equipment has a general right of access to his or her personal information under section 36 of MFIPPA. This right is recognized. However, Section 38(b) of MFIPPA, unjustified invasion of another individual's privacy, may apply.

8.7.1. Access to an individual's own personal information in these circumstances may depend upon whether affected third parties consent to the disclosure, or whether any exempt information may be severed from the record.

8.7.2. Redacted or blurring images may be required, however, the process can be costly. That cost of redacting video images will be forwarded directly to the requestor.

8.8. This procedure will be reviewed as needed.

8.9. The Information Technology Division shall respond to any inadvertent disclosures of personal information based on direction provided by the Town Clerk. Any breach of this policy shall be reported to the Office of the Town Clerk.

9. TRAINING:

9.1. All staff who have access to video security will receive training in accordance with the roles and responsibilities under this policy. This training may be provided in person, or by a multi-media device.

9.2. All staff at Town sites will receive training on video security, the Town's obligations, their responsibilities under MFIPPA, and how and if they may access video footage. This training will be carried out by the Office of the Town Clerk.

10. AUDITS:

10.1. Although developing policies, procedures and providing training to all staff is a requirement under this procedure, it is also a requirement to ensure staff are complying with and have an understanding of their role(s).

10.2. To accomplish the above the Town commits to verifying compliance with the video security policy and procedures through audits. The Office of the Town Clerk will perform regular audits of access to the Video Security system.

Appendix “B”

Notice to the Public

From the Director of Corporate Services

Date

Re: Video Security

The Town of Niagara-on-the-Lake is equipped with a video surveillance system. The video security system is in all Town of Niagara-on-the-Lake facilities, properties, and at the Town head office.

The purpose of the video security system is to protect the security of the public, staff and the Town’s properties. It is also a deterrent and identification tool for vandalism, criminal, and other illegal activities at our facilities.

All information obtained by video security is confidential and will only be provided to law enforcement authorities when criminal or other illegal acts are suspected. All video-recorded material will be destroyed within thirty (30) days or earlier of being recorded unless it is used as part of an investigation.

All information is managed in accordance with the Town of Niagara-on-the-Lake policy for Video Security, the *Municipal Freedom of Information and Protection of Privacy Act,* (MFIPPA) and the *Municipal Act.*

For more information, please contact the Office of the Town Clerk, Corporate Services, Town of Niagara-on-the-Lake at 905-468-3266.

Regards

Kyle Freeborn
Director of Corporate Services/Treasurer

Appendix “C”

Instant Access Form

Part A- Video Information
Location: Copy Date: Location of Camera: Date of Incident: Security Period:

Part B: Destruction of Video Recorded Data Log
Date: Date of Destruction: Destruction by:

*NB: If video recorded material is on a portable device as required as part of an on-going investigation, it shall be retained for at least one year after the investigation is completed.
** If video images are released as part of a law enforcement investigation the Town shall maintain a copy of the released material in accordance with the retention schedule.

Appendix “D”

Video Request Form

Town of Niagara-on-the-Lake

The following information must be forwarded at the time of each video request to the Town of Niagara-on-the-Lake. Note: Recorded Camera footage is only kept for thirty days or less, depending on security system storage. The information may be sent to the Town of Niagara-on-the-Lake in an emails, voicemail or in the form below:

Mandatory Information for Video Requests:

Name and rank of Officer requesting information	
Date of request	
Badge Number	
Incident/Occurrence Number	
Location of incident	
Date and time of incident	
Time range for video capture	
Reason for request (i.e. for investigation)	
Description of what you are looking for (i.e. assault in front of building, theft of car)	
Describe the camera(s) you require access to, i.e. Town Hall front entrance	
Additional information that may assist the Town in fulfilling the request	
Number of copies made at the time of the request	
Name of person contacted by Law Enforcement (NRPS)	
Name of Director approving the request	
Name of employee that made the copies	
Signature of Employee	
Contact information of Employee	
Date copy made	
Date copy picked up	
Name and badge number of NRPS Officer picking up the record	
Signature of NRPS Officer	
For additional information please contact the Officer of the Town Clerk	

Appendix E

Notices should include:

“THIS AREA IS MONITORED BY VIDEO SECURITY CAMERAS (CCTV)”.

Surveillance cameras are in operation for the safety of the public and staff and for the protection of Town of Niagara-on-the-Lake property. Information is collected under the authority of the *Municipal Act*, and in compliance with the *Municipal Freedom of Information and Protection of Privacy Act,* (MFIPPA). For additional information please contact the Office of the Town Clerk at (905) 468-3266.

Appendix F:

Locations of Video Security

1. Town Hall 1593 Four Mile Creek Road, Virgil ON
2. Operations Building 2 Lorraine Street, Virgil ON
3. NOTL Arenas
    a. MCU Arena
    b. Centennial Arena
4. NOTL Community Centre 14 Anderson Lane, Niagara-on-the-Lake ON
    a. Public entrances, hallways, auditoriums, gyms and parking areas
    b. Café lobby and entrance
    c. Library main entrance and Parking
5. Virgil Splash Pad and Pavilions
6. Niagara-on-the-Lake Skatepark
7. Intersection of Niagara Stone Road and Anderson Lane: Rainbow Crosswalk