

Town of Greater Napanee CCTV Policy



Approval Date:	March 10, 2026	Resolution #	136/26
Revised Date:		Resolution #	
Review Scheduled:	2028		
Department:	Legislative Services	Contact:	Clerk
Approval Authority:	Council	Policy No:	LS-2026-02

1. Introduction

The Town of Greater Napanee recognizes the need to balance an individual’s right to privacy with the need to ensure the safety and security of Town employees, clients, visitors and property. While Closed Circuit Television (CCTV) cameras are installed for safety and security reasons, the Town’s CCTV systems must also be designed to minimize privacy intrusion. The Town is committed to the improvement of community safety, crime prevention, and the desirability of the town as a place for shopping, business and leisure.

Guided by a commitment to public safety, crime prevention and stewardship of publicly owned assets, the Town may, where warranted by law, use CCTV systems in municipally owned buildings, or at municipally operated facilities, parks and open spaces.

2. Purpose

This policy establishes controls for the Town’s CCTV Program by governing the use of CCTV Systems and CCTV Records owned or operated by the Town in accordance with the relevant provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

3. Scope

This policy applies to:

- a) All Town officers, employees and agents;
- b) Contractors and service providers who may work with or operate CCTV equipment for the Town;
- c) All CCTV equipment in the care and control of the Town;
- d) The collection, use, disclosure and disposal of information collected through CCTV technology.

This policy does not apply to:

- e) Video or audio recordings of council or committee meetings; or
- f) Camera equipment installed on Town vehicles or other mobile assets.

4. Definitions

Authorized Users means Town employees who have been approved by the CAO to operate CCTV equipment and who have received training consistent with the requirements of this policy.

Consistent Purpose means use of personal information in manner that the individual to whom the information relates might reasonably have expected in the circumstances.

Live Feed means viewing of data captured from audio-visual devices and/or CCTV equipment, whether or not these data are recorded in a file or not.

MFIPPA means the *Municipal Freedom of Information and Protection of Privacy Act* of Ontario.

Personal Information in accordance with Section 2 of MFIPPA, means recorded information about an identifiable individual, including:

- a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual.
- b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved.
- c) any identifying number, symbol or other identifier assigned to the individual.
- d) the address, telephone number, fingerprints or blood type of the individual.
- e) the personal opinions or views of the individual except if they relate to another individual.
- f) 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.
- g) the views or 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 Impact Assessment means a written assessment that identifies the type of personal information intended to be collected and used, legal authority for its collection and use, employee positions that will have access to the

information, and protection measures that will be put in place to safeguard the information from unauthorized use or disclosure.

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.

Town means the Corporation of the Town of Greater Napanee.

CCTV Record means a video or still image created from the Town's CCTV system.

CCTV System means a collection of hardware and software components that enables centralized recording, observation and archiving of CCTV Records.

5. Responsibilities

5.1. Council

Council is responsible for:

- a) Approval of this policy and any amendments; and
- b) Approval of service levels for processing internal and law enforcement requests for CCTV records.

5.2. Chief Administrative Officer (CAO)

Responsibility and authority is delegated to the CAO to:

- a) Provide oversight and ensure compliance with this policy by all Town employees;
- b) Review and respond to alleged privacy breaches regarding the use of the CCTV system;
- c) Approve requests to establish Authorized Users, and define criteria for Authorized Users by way of management directive; and
- d) Review and approve Privacy Impact Assessments, in conjunction with IT, the Clerk, and the affected Department Head.

5.3. Clerk

Responsibility and authority is delegated to the Clerk to:

- a) Ensure the CCTV Program is compliant with MFIPPA;
- b) Respond to requests for access to CCTV Records under MFIPPA; and
- c) Ensure this policy is reviewed a minimum of once per Council term and when there are changes to relevant privacy laws or guidelines.

5.4. Manager of Information Technology (IT)

Responsibility and authority is delegated to the Manager of IT to:

- a) Assess equipment and system requirements and make necessary arrangements for purchase and installation;
- b) Take all reasonable precautions to ensure that CCTV equipment is secure and that unauthorized individuals are prohibited from reviewing or accessing information;
- c) Maintain records associated with the CCTV Program, including audit logs, device locations, and authorized users;
- d) Implement appropriate training and control measures for Authorized Users;
- e) Make recommendations on improvements to this Policy and to the CCTV Program; and
- f) Train authorized users in operating the CCTV system.

5.5. Management Staff

Responsibility and authority is delegated to Management Staff to:

- a) Authorize the installation of CCTV Equipment on municipal property under their supervision;
- b) Ensure mandatory public notice signage is installed which provides reasonable and adequate warning that CCTV may be in operation in locations under their supervision;
- c) Document the rationale for the installation of CCTV equipment;
- d) Submit a Privacy Impact Assessment and usage case for any proposed live viewing of CCTV footage; and
- e) Ensure internal requests for records are necessary for the performance of the requester's duties in the discharge of their functions.

5.6. Authorized Users

Responsibility and authority is delegated to Authorized Users to:

- a) Retrieve and provide access to CCTV Records in response to requests made under this policy and in accordance with any service levels as may be established by the CAO.

5.7. Employees

All Town employees with access to the CCTV System or Records are responsible to:

- a) Understand and adhere to this policy; and
- b) Report any observed or suspected privacy breaches in accordance with this policy.

6. Policy

6.1. Acceptable Use

- a) CCTV Systems may be used to:
 - i. View live feed, in limited and specific circumstances;
 - ii. Review CCTV records;
 - iii. Collect anonymized data to aid decision making, such as traffic volume or parking vacancy rates; and
 - iv. Extract and archive CCTV records.

- b) Live feed viewing by the Town shall only be permitted in the following circumstances, subject to a privacy impact assessment:
 - i. System maintenance carried out by the IT Department; and
 - ii. For the protection of employee health and safety or municipal infrastructure, in accordance with a video access business case that has been approved by the Department Head, IT Department, and the Clerk.

- c) CCTV Records shall be reviewed, extracted, or archived only for the purposes intended by the Town, including but not limited to:
 - i. System maintenance carried out by the IT Department;
 - ii. Investigation of reported incidents; and
 - iii. Viewing events in areas that require recordkeeping, as established in a departmental video access business case.

- d) Incidents shall be investigated only for the purposes intended by the Town, including but not limited to:
 - i. detecting, deterring, and investigating unlawful activity, which includes possible contraventions of any federal or provincial law or municipal by-laws;
 - ii. investigating and resolving claims of personal injury or damage to assets, and other legal claims; or
 - iii. investigating and resolving public complaints received by the Town or matters that may give rise to a customer complaint being received by the Town.

- e) Logs shall be kept of all instances of access to and use of CCTV Records.

- f) Use of CCTV Systems and CCTV Records is subject to audit.

- g) Access to CCTV Systems shall be restricted to authorized Users.

6.2. Notice of Collection of Personal Information

- a) The Town's collection of personal information as CCTV Records is

authorized through this Policy and is intended to specifically protect:

- i. The public assets of the municipality;
 - ii. The economic, social, and environmental well-being of the municipality;
 - iii. The health, safety and well-being of persons;
 - iv. Services and things the municipality is authorized to provide; and
 - v. Persons and property.
- b) The Town shall provide notice of its collection of personal information in the form of signage visible to members of the public. Signage shall be placed to provide the community reasonable an adequate warning about the use of CCTV by being:
- i. Clearly written;
 - ii. Prominently displayed at pedestrian entrances and interior walls of buildings where recording devices are installed; and
 - iii. Prominently displayed at pedestrian and vehicle entrances to public spaces where recording devices are installed.
- c) In accordance with Section 29(2) of MFIPPA, at least one sign in each location shall include the following information:
- i. The legal authority for the collection of personal information;
 - ii. The principal purpose(s) for which the personal information is intended to be used; and
 - iii. Contact details for further information.
- d) A map showing the approximate areas covered by CCTV is attached to this Policy as Appendix A.
- e) The current approved signage form is attached to this Policy as Appendix B.

6.3 Procedures and Principles of CCTV Use

- a) The CCTV usage procedures shall be performed based on the following principles:
- i. CCTV use shall be conducted in accordance with all applicable law, specifically Section 28(2) of MFIPPA;
 - ii. CCTV use shall be conducted in a professional, ethical, and legal manner;
 - iii. Authorized Users shall be appropriately trained and supervised in the responsible use of the CCTV equipment;
 - iv. The CCTV system shall not monitor individuals in any manner which would constitute a violation under the Ontario Human Rights Code (OHRC); and
 - v. Records obtained through the CCTV system shall be released only according to the standards set by MFIPPA and other

applicable law. The recordings shall be handled in a manner that provides continued security of the recorded information.

- b) The benefits of CCTV to the public shall be weighed against an individual's right to be free of unwarranted intrusion.
- c) The benefits of CCTV to the organization shall be weighed against an individual's and employee's right to be free of unwarranted intrusion.
- d) A process is in place to allow the public to make a complaint about the CCTV system through the Clerk's Office and a process is in place to allow the employees to make a complaint about the CCTV system through the Manager of Human Resources.
- e) Access to the recorded information is only permitted in accordance with MFIPPA, other applicable law, and this Policy.
- f) Live viewing is restricted to time periods when there is a demonstrably higher likelihood of safety and security concerns involving employees, the public or corporate assets, and where a privacy impact assessment has been completed and approved for the specific use.
- g) Live feed monitors are turned off when not in use.
- h) Live feed monitors are located in places only visible to and accessible by Authorized Users.

6.4. Privacy Considerations – CCTV Infrastructure

CCTV Systems shall only record Town property and publicly available outdoor spaces. In addition, in order to reduce the privacy impact to residents and facility users, at minimum the following requirements shall be followed:

- a) CCTV Systems shall not be configured to collect audio records, as recording audio may constitute "wiretapping" in violation of the Criminal Code of Canada.
- b) The Town shall not enable the use of facial recognition software through CCTV Systems without an amendment to this policy and completion of a privacy impact assessment and business case justifying its use.
- c) Recording Devices shall not monitor areas where customers, staff and the community have a higher expectation of privacy, including but not limited to the interior of washrooms, showers, and change rooms.
- d) Recording Devices shall not monitor residential areas that are not generally observable by the community from a public space.

- e) Recording Devices that monitor any buildings not owned by the Town shall digitally mask any visible interiors of those buildings, including but not limited to doors and windows.
- f) Recording Devices shall be installed only where they are expected to be the most effective to community safety efforts and Town operating procedures, including municipal facilities, municipal parks and public spaces, the downtown core streets and sidewalks, and major intersections.
- g) Remotely adjustable Recording Devices shall not be manipulated to monitor areas that are not intended to be monitored by the Town.

6.5. Records Access Procedures

The right to create or view CCTV Records is strictly limited and must be undertaken as follows:

- a) Public requests: Records related to public requests for disclosure shall be released by the Clerk, or their designate, upon a written request made through the freedom of information (MFIPPA) process.
 - i. 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.
 - ii. Any facial features will be blurred prior to the release of video records made under a freedom of information request.Records transmitted under MFIPPA will normally be sent through a secure time limited link.
- b) Law enforcement requests: Requests from Law Enforcement agencies will be processed in accordance with Section 6.6 of this Policy.
- c) Internal requests: Records related to internal investigations shall be created by the IT Department on receipt of a written request from the appropriate Department Head. Internal records shall only be retrieved for the purposes of:
 - i. investigations of incidents involving the safety or security of people, facilities, or assets;
 - ii. providing evidence as required to protect the Town's legal rights;
 - iii. investigating an incident or allegation of employee misconduct;
 - iv. investigating an incident involving an insurance claim; or
 - v. a consistent purpose.

Copies of records retrieved for an internal purpose will be reviewed by the requesting department head and either destroyed or retained by the Department Head in accordance with the records management requirements of the associated access purpose (i.e. insurance claim,

investigation, etc.).

- d) Where an internal request for CCTV records is made in the context of a workplace investigation involving Town employees, the request must be submitted by the Manager of Human Resources or the CAO.
- e) For all CCTV record retrieval, the IT Department shall log the following information as an Access Log Record:
 - i. The date and time of the original, recorded incident, including the location/number of the applicable camera.
 - ii. The identify of the person making the request.
 - iii. The case file number associated with the request.
 - iv. A description of the circumstances justifying the disclosure; and
 - v. The date the record was provided and the means of disclosure.
- f) The Town shall use the IT Department E11 or similar ticketing system to record and track all internal CCTV record requests.
- g) The Town shall use a separate ticketing system for tracking all law enforcement CCTV record requests.
- h) All external requests shall be directed to the MFIPPA process, with the exception of law enforcement, which shall be directed to the law enforcement process.
- i) If a video record containing personal information is improperly disclosed or is suspected to have been disclosed to an unauthorized person, the employee who is aware of the disclosure must immediately inform their manager, who will inform the Clerk and/or CAO as applicable in accordance with the privacy breach requirements.

6.6. Law Enforcement Records Requests

- a) The Town may disclose a copy of a video recording to a law enforcement agency only in the following circumstances:
 - i. Law enforcement approaches a Town agency or institution with a warrant requiring the disclosure of the footage, as per section 32(e) of the MFIPPA, or
 - ii. Law enforcement approaches a Town agency or institution without a warrant and requests disclosure of the footage to aid in an investigation from which a proceeding is likely to result, as per section 32(g) of the MFIPPA. Such requests shall be submitted using the form attached to this Policy as Appendix C, or
 - iii. Town employees observe an illegal activity on Town property and disclose the potential availability of footage to law enforcement to aid in an investigation from which a proceeding is likely to result, as per section 32(g) of the MFIPPA.

- b) Live viewing or use of any AI-assisted CCTV tools, including facial recognition, by Law Enforcement will be permitted on receipt of a warrant requiring such disclosure of the footage. In such cases, the requirements of Section 6.3 (g) and (h) shall apply.
- c) Records transmitted to law enforcement will normally be sent via a secure link through an evidence submission portal.
- d) Responses to law enforcement requests will be processed during regular business hours, which are Monday – Friday, 8:30 a.m. to 4:30 p.m., with consideration of the following service standards and constraints:
 - i. Same day footage requests are subject to the technical delays of the CCTV system where footage is not downloaded until up to 24 hours after it has been captured.
 - ii. The Town will deem a CCTV retrieval completed at the time that a file upload is initiated into a law enforcement digital evidence system, as the volume of footage requested has a direct impact on the time required for file transmission.
 - iii. Simple records requests which involved three or fewer camera locations and a defined retrieval window will normally be processed within two business days.
 - iv. Complex records requests which involve multiple camera locations and/or multiple time windows will normally be processed within five business days.
 - v. Records requests will be prioritized based on the following considerations:
 - The incident date in relation to the 30 day retention period;
 - Requests to aid in the identification of an alleged incident or offender to be prioritized over requests to aid in providing supporting evidence where charges have already been laid; and
 - Requests related to serious criminal offences will be prioritized over requests related to lower level offences.
 - vi. Town staff will retrieve records based on a defined criteria related to time and location, but will not perform live analysis or active searching on behalf of law enforcement.
- e) Pursuant to s. 32(g) of MFIPPA, the Town cannot disclose personal information to a law enforcement agency when the agency cannot provide definite and focused investigative information as to why the disclosure is needed. This can include the type of offence that is suspected, confirmation that the matter is expected to lead to legal proceedings, and a specific case number.

- f) The Town will not disclose information if the request parameters are so broad as to capture large volumes of personal information unrelated to the enforcement purpose. Such requests will be referred to the Clerk for assessment and a decision regarding whether the records may be released or if a warrant or legal order is required.

6.7. Records Retention and Disposition

- a) CCTV information that is not subject of an authorized request for access will be considered transitory and will be automatically erased by the system by being overwritten every thirty (30) days.
- b) CCTV Records that have been extracted as part of an investigation shall be stored for the duration of the retention period recommended by MFIPPA, being a minimum of 1 year.

6.8. Policy Review

- a) The Manager of IT and the Clerk shall review this policy annually to ensure effectiveness and compliance with current business processes, or sooner if based on legislative changes.
- b) This policy shall be reviewed by Council at least once per term.

7. Enforcement

Users shall comply with all Town policies, procedures and standards while using CCTV Systems and Records, including but not limited to all confidentiality policies. Employees who breach this policy, or the relevant legislation, may be subject to disciplinary action and/or civil liability.

Users shall comply with all laws and regulations of applicable jurisdictions while using CCTV Systems and Records, including but not limited to:

- a) The Criminal Code of Canada
- b) The Canadian Charter of Rights and Freedoms
- c) The Canadian *Human Rights Act*
- d) The Ontario *Human Rights Act*
- e) The Ontario *Municipal Freedom of Information and Protection of Privacy Act*

Users shall comply with any audit or investigation by the Town surrounding their use of CCTV Systems and Records,

8. Related Documents

Municipal Freedom of Information and Protection of Privacy Act

IPC Guidelines for the Use of Video Surveillance

IPC Guidelines for Disclosure of Personal Information to Law Enforcement

Appendices

Appendix A – Map of CCTV System

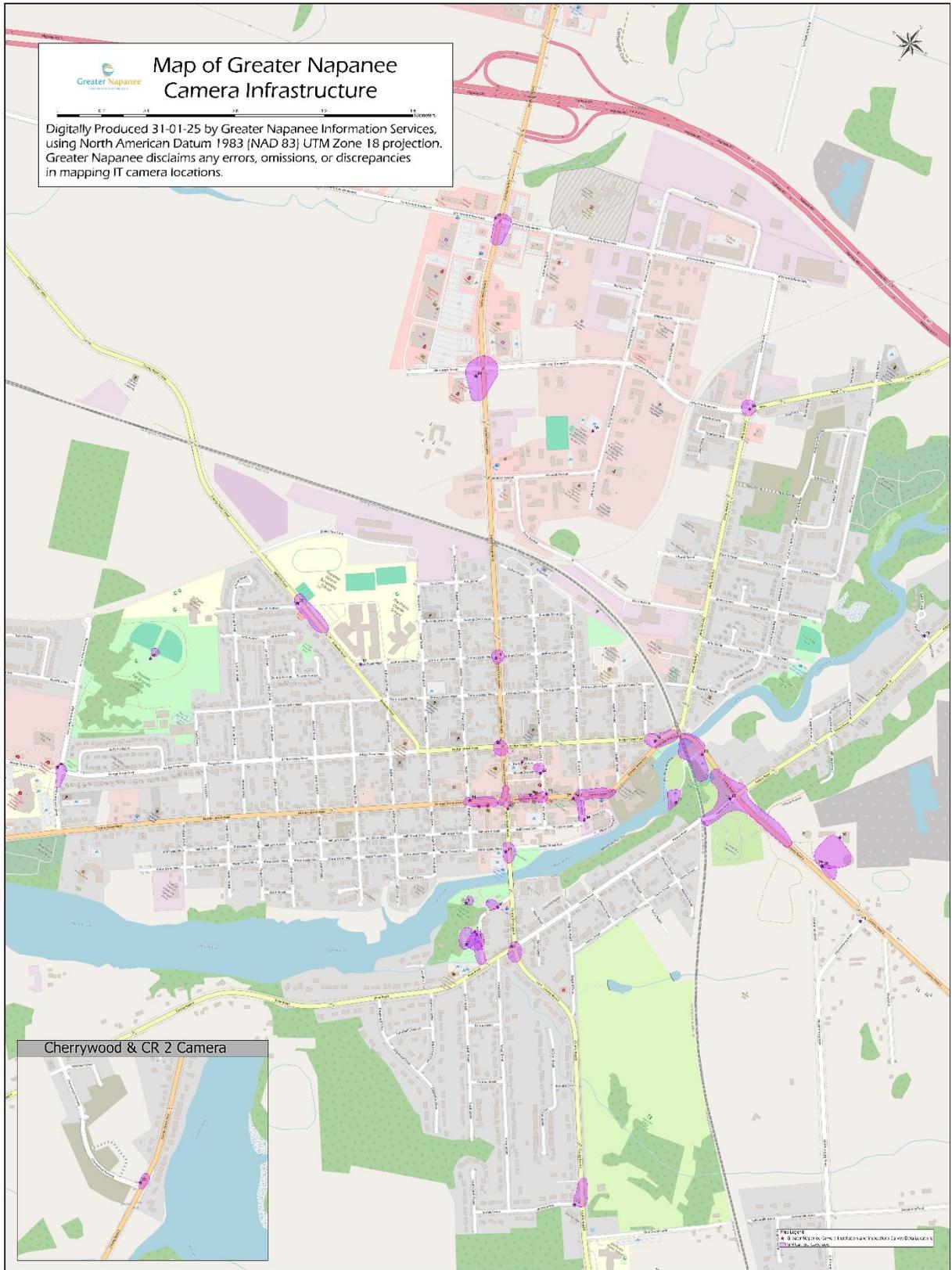
Appendix B – Notice of CCTV Sign

Appendix C – Law Enforcement Record Request Form

Revision History

Date	Number	Description
March 2026	LS-2026-02	Expanded Policy
April 2015	N/A	Downtown CCTV Program Policies & Procedures (Internal Document)

Appendix A-1 – CCTV Coverage Map



Appendix A-2 – List of Town Facilities with CCTV Installed

Exterior and Limited Interior

- Administration Building – 99 Advance Ave
- Arena – 16 McPherson Drive

Exterior Only

- AL Dafoe Water Plant – 75 East Street
- Water Pollution Control Plant – 300 Water Street
- Roblin Waste Disposal Site – 232 Roblin Road
- South Fredericksburgh Waste Disposal Site – 651 Road 1
- Selby Public Works Yard – 1599 County Road 41
- Napanee Public Works Yard – 8321 County Road 2
- Train Station – 301 John Street
- Town Hall – 124 John Street

To promote safety this area is under video surveillance

Images may be recorded and/or monitored



The personal information collected by the municipal cameras within the Town is collected under the authority of the Municipal Act, 2001 and the Town's Corporate Policy on Video Surveillance. This information is used for the purpose of promoting public safety and protection of municipal property

Inquiries about the use and collection of this information may be directed to the Town Clerk at 613-354-3351 or 99 Advance Ave.

Appendix C – Law Enforcement Record Request Form

The following information is being requested under section 32(g) of the *Municipal Freedom of Information and Protection of Privacy Act* which allows for the disclosure of records containing personal information for the purposes of aiding a law enforcement investigation. This form is not to be used for requests for third party or confidential information held by the Town of Greater Napanee. All such requests are to be referred to the Town Clerk or designate.

Please be advised that CCTV video footage is only available for 30 days from date of recording unless a request has been received to place a hold on specific footage.

Requester Information

Name of Requester:	Badge Number:	File Reference Number:
Phone:	Email:	Record Receipt Method:

Footage Information

Offence	Section & Statute:	Have Charges been Laid? <input type="checkbox"/> Yes <input type="checkbox"/> No
Date of Incident	Time Frame of Incident	Location of Incident
Description of Incident		
Other Details, if applicable		

Acknowledgement

I certify that:

- a) The information above is accurate and correct to the best of my knowledge;
- b) I have the authority to collect the information requested on behalf of the agency noted for the purpose(s) specified.
- c) This information is requested in accordance with Section 32(g) of the Municipal Freedom of Information and Protection of Privacy Act, as the information will aid in an investigation undertaken with a view for a law enforcement proceeding or from which a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

Signature

Date