Policy Name: Video Surveillance Policy	Policy No: S203-19
Committee approval date:	-
Council approval date:	-
Revision date(s):	-
Department/Division:	Clerk's

1. Purpose

The purpose of this Policy is to establish guidelines for the Video Surveillance Program of the Town of Pelham (the "Town") in compliance with the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56 ("*MFIPPA"*), the *Municipal Act, 2001,* S.O. 2001, c. 25 (*"Municipal Act, 2001"*), and the Information and Privacy Commissioner of Ontario (IPC) Guidelines for the Use of Video Surveillance.

This Policy applies to Video Surveillance Systems located on Town property and ensures that their use by the Town is conducted in a manner that respects individuals' privacy while enhancing public safety and security.

2. Policy Statement

The Town is committed to enhancing the safety and security of the public, its employees, and its property while balancing an individual's fundamental right to privacy. Accordingly, the Town is committed to full compliance with provincial privacy laws regarding the notice, collection, access, use, disclosure, retention and disposal of personal information. This includes adherence to data minimization principles, which, for video surveillance, entails limiting the amount of personal information collected and retained to what is necessary to fulfill the purposes of the lawfully authorized activity.

3. Definitions

"Authorized Use" means disclosure of Video Surveillance System Footage (i) in response to a law enforcement request made pursuant to section 32 of *MFIPPA*; (ii) when required by law, such as a court order or access request made under sections 32 and 36 of *MFIPPA*; and/or (iii) where necessary to protect public safety and authorized under *MFIPPA* or a Town policy for this purpose.

"Authorized Staff" means employees of the Town who are authorized to review Video Surveillance System Footage.

"Clerk" means the Clerk of the Town or designate.

"Head" means the Clerk that has been designated by Council to act as the head of the Town for the purposes of *MFIPPA*.

"Information and Privacy Commissioner (IPC)" means the independent officer of the Ontario Legislature that provides oversight on Ontario's access and privacy laws, ensuring that personal information remains private and secure while granting the public the right to access government-held information.

"Personal Information" means personal information as defined in section 2 of *MFIPPA*, namely, recorded information about an identifiable individual, including but not limited to information relating to an individual's race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital status.

"Privacy Analysis" means a checklist with specific privacy-related questions to help inform the Privacy Impact Assessment and assist the Town in determining if expansion or modification to the current Video Surveillance Program is necessary.

"Privacy Breach" means any loss or theft of Personal Information and/or any collection, disclosure, or use of Personal Information that occurs without authority and in a manner that does not comply with Ontario's privacy laws.

"Privacy Impact Assessment (PIA)" means a risk management tool used by the Town to identify the actual or potential effects that a proposed or existing information system, technology, program, process or other activity may have on an individual's privacy.

"Town Facility" means any land, building, or structure owned or occupied by the Town that is open to the public, including but not limited to fields, parks, pools, splash pads, arenas, gymnasiums, multi-use community rooms, and parking areas.

"Unauthorized Use" means any accessing or disclosure of Video Surveillance System Footage that is not an Authorized Use.

"Video Surveillance Program" means a system that uses cameras to monitor Town Facilities and infrastructure to enhance safety, security, and compliance, and that includes policies on camera use, data storage, access, and privacy to ensure responsible and lawful operation.

"Video Surveillance System(s)": Any recording system, physical or other mechanical, electronic, digital, or wireless surveillance system or device that enables continuous or periodic video recording, observing or monitoring of individuals in Town Facilities.

"Video Surveillance System Footage" means the video recording(s) captured by a Video Surveillance System.

4. General Provisions

4.1 Legal Authority and Justification

Under the Municipal Act, 2001, the town has authority to provide services necessary or desirable for the health, safety, and well-being of persons and the protection of Town assets. This includes security measures such as Video Surveillance Systems.

The Town has authority under section 28 of *MFIPPA* to collect Personal Information, including Video Surveillance System Footage, where the collection is (i) expressly authorized by statute; (ii) necessary for the proper administration of a lawfully authorized activity; or (iii) used for law enforcement purposes.

In keeping with these legal requirements, the Town will use Video Surveillance Systems only where necessary for public safety, crime prevention, or the protection of Town assets. Additionally, before implementing a Video Surveillance System at any Town Facility, the Town will assess whether less intrusive alternatives have been considered and determined to be inadequate. This assessment is discussed further in section 4.6 of this Policy.

4.2 Notice of Collection and Public Awareness

The Town is required to provide notice of the collection of Personal Information to individuals whose information is collected. Section 29 of *MFIPPA* provides that individuals must be informed of (i) the legal authority for the collection; (ii) the principal purpose or purposes for which the Personal Information is intended to be used; and (iii) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

The Town will provide notice of the use of Video Surveillance Systems in Town Facilities by posting signage at the perimeter of all monitored areas and at key locations within monitored areas. The signage will have clear, language-neutral graphical descriptions of the use of a Video Surveillance System and will provide the information prescribed by section 29 of *MFIPPA*.

The Town's approved signage is attached as Appendix "A" to this Policy.

To further facilitate public awareness, the Notice of Collection of Personal Information and this Policy will be available on the Town's website at www.pelham.ca/video.

4.3 Location and Use of Video Surveillance System

The Town will implement Video Surveillance Systems in Town Facilities only where there is a demonstrated need for the use of a Video Surveillance System for public safety, crime prevention, or the protection of Town assets.

The Town will not install any component of a Video Surveillance System in any area of a Town Facility where individuals have a high expectation of privacy, such as washrooms or changerooms.

The Town currently uses Video Surveillance Systems in the Town Facilities listed in Appendix "B" to this Policy. The Town is satisfied that the requirements of this Policy are met at all current locations.

4.4 Retention, Access, and Disclosure

Video Surveillance System Footage recorded at the Meridian Community Centre (MCC) will be retained for no more than fifteen (15) calendar days, unless required for an investigation or legal hold for actual or potential litigation or law enforcement purposes.

Video Surveillance System Footage recorded at any other Town Facility will be retained for no more than thirty (30) calendar days, unless required for an investigation or legal hold for actual or potential litigation or law enforcement purposes.

If Video Surveillance System Footage is subject to a law enforcement request, legal hold, or formal *MFIPPA* access request, it must be retained until the matter is resolved, as provided for in section 5 of *MFIPPA*.

Access to Video Surveillance System Footage is restricted to Authorized Staff with a legitimate need to review it or as provided for in section 31 of *MFIPPA*. Any employee who engages in Unauthorized Use is subject to disciplinary action.

Video Surveillance Footage may be disclosed only for an Authorized Use. Any disclosure must be documented by the Town in a log maintained by the Manager of Information Technology, which must include (i) the date and time of access, (ii) the person/entity requesting access, and (iii) the reason for disclosure.

Individuals may request access to Video Surveillance System Footage that contains their Personal Information by submitting a formal request under section 36 of *MFIPPA*. The Head will review requests to determine whether disclosure is permitted under the statute's privacy and law enforcement exemptions.

4.5 Security and Protection of Video Surveillance System Footage

MFIPPA regulations require the Town to define, document, and implement reasonable measures to prevent the Unauthorized Use of Video Surveillance System Footage. Accordingly, the Town will store Video Surveillance System Footage on secure devices equipped with encryption or other security measures to protect data integrity and maintained in controlled locations. The Town will also ensure that any contracts between the Town and third parties include privacy and security obligations to ensure compliance with this Policy when third-party service providers fall under any part of this Policy.

4.6 Public Consultation and Privacy Considerations

Prior to expanding the Town's current Video Surveillance Systems, the Town will conduct public consultations to gather input from the community on the necessity, scope, and potential impacts of surveillance. The Clerk's Department will post a Public Notice on the Town's website (www.pelham.ca) containing information on the proposed Video Surveillance System(s) and allow for a two (2) week commenting period for agencies and the public. Public comments will be delivered to the Clerk for review and consideration.

The Town will also undertake a Privacy Analysis and PIA before implementing any new or significantly modified Video Surveillance System to evaluate its necessity, proportionality, and effectiveness while considering alternative measures. PIAs will be conducted by the Clerk's Department in conjunction with the Manager of Information Technology and the manager(s) of the Town Facility/Facilities where the Video Surveillance System is present or proposed. The Town will ensure that privacy considerations, such as limiting the collection of Personal Information and data minimization principles, are incorporated into the design of, and operational procedures for, any new or significantly modified Video Surveillance System.

The Privacy Analysis Checklist is attached as Appendix "C" to this Policy and the PIA Report Template is attached as Appendix "D" to this Policy.

In the event of a Privacy Breach involving the Town's Video Surveillance Program, the Town will take the steps outlined in Appendix "E" to this Policy.

4.7 Review and Audits

The Manager of Information Technology will review the Video Surveillance Program every two (2) years to ensure compliance with this Policy and relevant legislation.

The Head may periodically conduct privacy audits of the Video Surveillance Program to assess compliance with section 4.1 of *MFIPPA* and ensure that privacy protections remain effective.

The Clerk's Department will review this Policy every two (2) years and update as necessary to reflect changes in legislation, technology, and municipal needs.

4.8 Roles and Responsibilities

All Town employees have a shared responsibility to implement and adhere to this Policy.

The Clerk is responsible for:

- directing compliance and resolving any conflicts with this Policy;
- administering and communicating this Policy broadly to all Town employees;
- establishing and approving procedural guidelines;
- responding to requests for disclosure of records under *MFIPPA* or applicable routine disclosure procedures;
- responding to requests from the public and employees about the collection, use, and disclosure of Personal Information captured by any Video Surveillance System;
- educating employees and the public on the collection, use, and disclosure of Personal Information through Video Surveillance Systems;
- coordinating PIAs and public consultations, as required;
- working with the department manager(s) and employee(s) in the event of an improper disclosure of Personal Information;

- responding to privacy complaints received through the IPC; and
- notifying the IPC in the event of a Privacy Breach, where appropriate.

The Manager of Information Technology (IT) is responsible for:

- operating and maintaining the Video Surveillance Systems;
- ensuring that the Video Surveillance System location document is kept up to date;
- ensuring Notice of Collection signs are posted at all Town locations that operate Video Surveillance Systems;
- providing access to the Video Surveillance System Footage to Authorized Staff as deemed necessary;
- maintaining the access log described in this Policy;
- the life cycle management of the Video Surveillance Systems, including the specifications, equipment standards, installation, maintenance, replacement and disposal;
- all technical and security aspects of Video Surveillance Systems as set out in this Policy;
- determining appropriate Video Surveillance System Footage storage methods and locations; and
- securely disposing of Video Surveillance System Footage after the applicable retention period expires.

Directors and Managers of the Town are responsible for:

- ensuring the appropriate use of the Video Surveillance Systems at Town Facilities for which they are responsible;
- ensuring that Notice of Collection signage at Town Facilities for which they are responsible is properly installed at and visible to the public at all times;
- notifying the Clerk when employee training is required;
- referring any requests for Video Surveillance System Footage from the public to the Clerk or designated employee;
- reporting any technical problems with the Video Surveillance Systems to the Manager of Information Technology (IT); and

- reporting any Privacy Breaches to the Clerk or designated employee.

All employees of the Town are responsible for:

- following this Policy and its related procedures in all circumstances;
- notifying their manager of Video Surveillance System Footage that may require a legal hold or be subject to an investigation;
- reporting to their manager any actual or suspected Privacy Breach;
- reporting to their manager any lack of visibility, damage, or unauthorized alterations to the Notice of Collection signage as shown in Appendix "A"; and
- reporting any issues with the Video Surveillance System at their location to their manager.

5. Attachments

Appendix A – Approved "Notice of Collection" Language and Signage

Appendix B – Video Surveillance System Locations

Appendix C – Privacy Analysis Template

Appendix D – PIA Report Template

Appendix E – Privacy Breach Management

To promote safety, this area is under video surveillance.

Notice of Collection:
Images and audio may be monitored and/or recorded.

Information collected by the use of video equipment in this area is collected under the authority of the *Municipal Act, 2001*, in accordance with the provisions of the *Municipal Freedom of Information and Protection of Privacy Act*.

For additional information, please contact the Clerk's Office.
20 Pelham Town Square | Fonthill ON | L0S 1E0
www.pelham.ca/video | 905-892-2607

Pelham
NIAGARA

Appendix “B”

Video Surveillance System	Location
1	Town Hall 20 Pelham Town Square, Fonthill
2	Fire Station 1 177 Highway #20 West Fonthill
3	Fire Station 2 766 Welland Road Fenwick
4	Marlene Stewart Streit Park 55 Park Lane, Fonthill
5	Centennial Park 989 Church Street, Fenwick
6	Meridian Community Centre 100 Meridian Way, Fonthill

Appendix "C"

Privacy Analysis Checklist

Project Information

- **Project Name:**
- **Department:**
- **Date of Assessment:**
- **Assessor(s):**
- **Project Lead:**

1. PERSONAL INFORMATION ASSESSMENT

Question	Yes	No	Comments/Actions Required
Does the project involve the collection, use, or disclosure of personal information?	☐	☐	
Is any of the personal information considered sensitive (e.g., financial)?	☐	☐	
Is the information collected directly from individuals?	☐	☐	
Is there a clear and lawful purpose for collecting personal information?	☐	☐	
Is there a legal authority for collecting, using, and disclosing the personal information?	☐	☐	
Is the minimum necessary personal information being collected for the purpose?	☐	☐	
Are individuals informed about the purpose and use of their personal information?	☐	☐	
Are individuals given the opportunity to provide consent where required?	☐	☐	

2. DATA HANDLING & SECURITY

Question	Yes	No	Comments/Actions Required
Are there established processes for securely storing personal information?	☐	☐	
Is access to personal information restricted to authorized personnel?	☐	☐	
Are audit logs in place to track access and changes to personal information?	☐	☐	
Are encryption and other security measures used to protect data?	☐	☐	
Is data transmitted securely (e.g., via encrypted email or secure portals)?	☐	☐	
Is personal information disposed of securely when no longer needed?	☐	☐	

3. INFORMATION SHARING & DISCLOSURE

Question	Yes	No	Comments/Actions Required
Is personal information shared with any third parties (e.g., vendors, contractors)?	☐	☐	
Are there agreements (e.g., contracts, MOUs) in place to ensure third parties comply with privacy laws?	☐	☐	
Is personal information only shared for lawful and necessary purposes?	☐	☐	
Are individuals informed about how their information may be shared?	☐	☐	
Are there mechanisms to ensure third parties securely store and dispose of personal information?	☐	☐	

4. INDIVIDUAL RIGHTS & PRIVACY COMPLIANCE

Question	Yes	No	Comments/Actions Required
Can individuals access and correct their personal information?	☐	☐	
Is there a process for responding to privacy complaints and inquiries?	☐	☐	
Are individuals provided with information on how their privacy is protected?	☐	☐	
Are policies and procedures in place to ensure compliance with applicable privacy laws (e.g., MFIPPA)?	☐	☐	

5. PRIVACY IMPACT & RISK MITIGATION

Question	Yes	No	Comments/Actions Required
Have potential privacy risks been identified?	☐	☐	
Have mitigation strategies been developed for identified risks?	☐	☐	
Are privacy risks documented and regularly reviewed?	☐	☐	
Are staff trained on privacy responsibilities and best practices?	☐	☐	
Has a Privacy Impact Assessment (PIA) been conducted?	☐	☐	

6. FINAL REVIEW & APPROVAL

- **Summary of Findings:** *(Briefly describe key risks, issues, and required actions)*
- **Recommendations:** *(List recommended steps to mitigate privacy risks)*
- **Approval Signatures:**
    - **Town Clerk: _____ Date: _____**

Appendix "D"

PRIVACY IMPACT ASSESSMENT (PIA) REPORT TEMPLATE

I. TITLE PAGE

- **Project Name**:
- **Department**:
- **Date**:
- **Prepared by**:

II. EXECUTIVE SUMMARY

Provide an overview of the project, key findings, recommendations, and any outstanding privacy impacts.

Key Points:

- Summary of the project purpose and scope.
- Major privacy risks and key findings.
- Recommended actions and mitigation strategies.
- Any remaining privacy concerns.

III. INTRODUCTION

Objective of the Project

Explain the purpose and goals of the project.

Purpose of the PIA Report

- Why the PIA was conducted.
- How it informs decision-making.
- The importance of privacy analysis.

Response Sought and Timelines

- What feedback/approval is needed.
- Deadlines for review and implementation.

IV. BACKGROUND

General Overview

Provide high-level context, including:

- PIA Process: Explain the purpose and outcomes of each phase (preliminary analysis, project analysis, privacy analysis).
- Scope: Define in-scope and out-of-scope elements.
- Glossary: Define specialized terms and acronyms.

V. PROJECT OVERVIEW

Project Summary

- Description of the project.
- Primary objectives and expected outcomes.
- Implementation details.

Accountability

- Identify key decision-makers and project leaders.

Related Initiatives and Linkages

- Connections to other programs, systems, or PIA reports.

Project Partners and Stakeholders

- Internal and external parties involved.

VI. PRIVACY ANALYSIS

Personal Information Involved

- Type of personal data collected.
- Scope and sensitivity of the information.
- Impact on individuals.

Legal Authority

- Laws, regulations, and policies governing the project.
- Relevant privacy legislation (e.g., MFIPPA).
- Agreements with third parties.

Privacy Roles and Responsibilities

- Who is responsible for privacy compliance?

Stakeholders

- Consultation processes and results.

VII. PROCESSES AND INFORMATION FLOWS

- Description of processes.
- How personal information is collected, used, retained, disclosed, and disposed of.
- Who has access to the data and their responsibilities.

VIII. PRIVACY IMPACT ANALYSIS

Findings

- Identified privacy risks.

Privacy Implications

- How the project affects privacy rights.

Recommendations

- Steps to mitigate risks and comply with regulations.
- Implementation plan with responsibilities and timelines.

IX. CONCLUSIONS

- Summary of key findings and outstanding risks.
- Impact of the project on privacy.
- Whether privacy risks can be mitigated or remain unresolved.

X. NEXT STEPS

- Follow-up actions and timelines.
- Approval and implementation of the mitigation strategy.

XI. APPROVAL

(Signatures of project leads and decision-makers to confirm understanding and acceptance of findings.)

- **Project Lead Name & Signature**
- **Approval Date**
- **Additional Approvals (if required)**

XII. ATTACHMENTS

Include supporting documents such as:

- Privacy legislation references.
- List of reviewed documents and interviews.
- Roles and responsibilities chart.
- Information flow diagrams.
- Privacy Analysis Checklist.
- Summary of recommendations and action items.

Appendix “E”

Privacy Breach Management:

1. **Contain the Breach**
    a. Secure and limit access to the affected surveillance footage.
    b. Shut down or disable the compromised system if necessary.
    c. Retrieve and secure any improperly disclosed or accessed video recordings.
2. **Assess the Breach**
    a. Determine what Personal Information was involved and how the breach occurred.
    b. Identify the individuals affected and assess the risk of harm.
    c. Review logs and access records to identify unauthorized access.
3. **Notify Affected Individuals**
    a. If the breach poses a risk of harm, notify affected individuals as soon as possible.
    b. Provide details on what happened, what information was compromised, and any steps they can take to protect themselves.
    c. If law enforcement is involved, coordinate notification efforts accordingly.
4. **Notify the IPC (If Applicable)**
    a. If the breach is significant (e.g., large-scale exposure, sensitive personal data), notify the IPC.
    b. Include details on the scope of the breach, mitigation measures, and corrective actions taken.
5. **Investigate and Implement Corrective Measures**
    a. Identify the root cause of the breach.
    b. Strengthen security protocols (e.g., encryption, access controls, retention policies).
    c. Provide staff training on privacy protection and breach prevention.
6. **Review and Update Policies**
    a. Conduct an internal review of video surveillance policies and procedures.
    b. Implement new safeguards if needed to prevent future breaches.
    c. Ensure ongoing privacy audits and monitoring.