

Municipality of *Bluewater*

Policy and Procedure

Policy:	Video Taping and Live Broadcasting
Effective Date:	October 7, 2024
Approved By:	By-law 83-2024
Supersedes:	N/A

Purpose:

The Municipality of Bluewater recognizes that video surveillance technology has the potential to infringe upon an individual's right to privacy. While video surveillance technology may be required for legitimate operational purposes, its use must be in accordance with the provisions of the Municipal Freedom of Information and Protection of Privacy Act (the Act).

Video security surveillance systems are a resource used by The Corporation of the Municipality of Bluewater at selected sites within the jurisdiction of the Corporation or property owned or leased by the Corporation within the boundaries of Bluewater. In the event of a reported or observed incident, the review of recorded information may be used to assist in the investigation of the incident.

This policy will provide guidelines designed to assist Bluewater Departments that have identified an appropriate use for video surveillance technology, to manage records that may be created using this technology in a manner that complies with the Act, and records management requirements.

Definitions:

Council – Council for the Corporation of the Municipality of Bluewater.

Manager – The appointed head of each department or their designate as identified in the Municipality of Bluewater organizational chart or through delegation.

Personal Information – Is defined in Section 2 of the Municipal Freedom of Information and Protection of Privacy Act, 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 surveillance system displays these characteristics of an identifiable individual or the activities in which he or she is engaged, its contents will be considered "personal information" under the Act.

Reception Equipment – refers to the equipment or device used to receive or record the personal information collected through a video surveillance system, including a camera

or video monitor or any other video, audio, physical or other mechanical, electronic or digital device.

Record – means any record of 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.

Staff – the CAO and all officers, directors, managers, supervisors, and all employees, whether full-time, part-time, contract, seasonal or volunteer employees, as well as agents and consultants acting in furtherance of Bluewater’s interests.

Storage Device – refers to a videotape, computer disk or drive, CD ROM, computer chip or other device used to store the recorded data or visual, audio or other images captured by a video surveillance system

Bluewater – The Corporation of the Municipality of Bluewater.

Video Surveillance – refers to a video, physical or other mechanical electronic or digital surveillance system or device that enables continuous or periodic video recording, observing or monitoring of personal information about individuals in open, public spaces (including streets, highways, parks).

Scope and Applicability:

These guidelines do not apply to covert surveillance used for law enforcement purposes. In those circumstances, either a statutory authority exists and/or the authority for the surveillance is lawfully obtained through a search warrant.

Covert surveillance is conducted through the use of hidden devices. If covert surveillance is not implemented pursuant to the conditions in the preceding paragraph, extra diligence in considering the use of this technology is required. However, covert surveillance is beyond the scope of this policy.

These guidelines do not apply to videotaping or audiotaping Bluewater Council or Committee meetings.

Policy:

It is the policy of The Corporation of the Municipality of Bluewater to utilize video surveillance to ensure the security of individuals, assets and property.

Guidelines: the following guidelines are applicable to all Bluewater Departments:

Designated Responsibilities:

- The Manager of Corporate Services or designate is responsible for ensuring the establishment of departmental procedures for video surveillance equipment in accordance with this policy. The manager or designate is responsible for the life-

cycle management of authorized video security surveillance systems [specifications, equipment standards, installation, maintenance, replacement, disposal and related requirements (e.g. signage)] including:

- Documenting the reason for implementation of a video surveillance system at the designated area.
 - Maintaining a record of the locations of the reception equipment.
 - Maintaining a list of personnel who are authorized to access and operate the system(s).
 - Maintaining a record of the times when video surveillance will be in effect.
 - Posting a Notice of Collection of Personal Information (Refer to Section 4).
 - Assigning a person responsible for the day-to-day operation of the system in accordance with the policy, procedures and direction/guidance that may be issued from time-to-time.
- Bluewater employees and service providers shall review and comply with the policy and the Act in performing their duties and functions related to the operation of the video surveillance system.
 - Bluewater employees may be subject to discipline if they knowingly or deliberately breach the policy or the provisions of the Act or other relevant statutes.
 - Where Bluewater has a contract with a service provider, the contract shall provide that failure by the service provider to comply with the policy or the provisions of the Act is considered a breach of contract leading to penalties up to and including contract termination. Employees of institutions and employees of service providers should sign written agreements regarding their duties under the policy and the Act, including an undertaking of confidentiality.

Considerations:

- Prior to installation of video surveillance equipment, the responsible department must consider the following:
 - The use of each video surveillance camera should be justified on the basis of security based on verifiable, specific reports of incidents of crime or significant safety concerns or for crime prevention. Video cameras should only be installed in identified public areas where video surveillance is a necessary and viable detection or deterrence activity.
 - An assessment of the effects that the proposed video surveillance system may have on personal privacy should be conducted in an attempt to mitigate any adverse effects. Privacy intrusion should be minimized to that which is absolutely necessary to achieve its required, lawful goals.
 - A requirement that any agreements between the Municipality and service providers state that the records dealt with or created while delivering a

video surveillance program are under Bluewater's control and subject to privacy legislation (MFIPPA).

- A requirement that employees and service providers (in the written agreement) review and comply with the policy and the Act in performing their duties and functions related to the operation of the video surveillance system.

Installation and Placement:

- Video surveillance equipment should never monitor the inside of areas where the public and employees have a higher expectation of privacy such as change rooms, washrooms or other similar areas where personal privacy and/or confidentiality is expected.
- Equipment should be installed in a strictly controlled access area. Only controlling personnel should have access to the access area and the equipment.
- Equipment should be installed in such a way that it only monitors those spaces that have been identified as requiring video surveillance.
- Adjustment of the camera position should be restricted, if possible, to ensure only designated areas are being monitored.
- Video surveillance should be restricted to periods when there is demonstrably a higher likelihood of crime being committed and detected in the area under surveillance. Video surveillance may occur on a continuous basis in areas where deemed necessary.

Notification:

- The public should be notified of the existence of video surveillance equipment by clearly written signs prominently displayed at the entrances, exterior walls, interior of buildings and/or perimeter of the video surveillance areas. Signs shall be in English.
- Signage must satisfy the notification requirements under section 29(2) of the Act, which include:
 - Informing 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; and
 - The title, business address and telephone number of someone who can answer questions about the collection;
 - The following is suggested wording for use in building signage, based on a minimum requirement of the IPC:
 - "THIS AREA IS MONITORED BY VIDEO SURVEILLANCE CAMERAS. Please direct inquiries regarding the collection of personal information to Bluewater's Clerk at the Municipal Offices, 14 Mill Avenue, 519-236-4351." This wording shall be provided in English.

- Bluewater's Video Surveillance Policy and the Departmental procedures that have been put in place can be obtained via Bluewater's Clerk.

Access, Use and Disclosure:

- Information collected by way of video surveillance systems may only be used for the purposes of the stated rationale and objectives set out to protect public safety or to detect and deter criminal activity and vandalism. Information should not be retained or used for any other purposes.
- All tapes or other storage devices that are not in use should be dated, labeled and stored securely in a locked container located in a controlled access area.
- Access to the storage devices should only be by authorized personnel. Logs should be kept of all instances of access to, and use of, recorded material to enable a proper audit trail. The personal information recorded by video surveillance is subject to access and privacy legislation. An individual whose personal information has been collected by a video surveillance system has a right of access under Section 36 of the Municipal Freedom of Information and Protection of Privacy Act. Access will depend upon whether an exemption applies and if exempt information can be reasonably severed from the record.
- Only the CAO, Manager of Corporate Services, Department Manager (or designate of any), or Municipal Solicitor, may review the information. Circumstances, which would warrant review, will normally be limited to an incident that has been reported/observed or to investigate a potential crime.

Retention:

- Unless otherwise established, the retention period for information that has not been viewed for law enforcement or public safety purposes shall be fourteen (14) calendar days for digital systems. Once the retention period is met, all tapes must be erased and reused or securely disposed of (shredded, burned or degaussed). Bluewater may use self-erasing, re-setting systems which are pre-set to a designated time period.
- When recorded information has been viewed for law enforcement or public safety purposes, the retention period shall be a minimum of one (1) year from the date of viewing. However, this information may be retained for a period longer than one year if legal action or prosecution which relies on this evidence is ongoing.
- Bluewater will store and retain storage devices required for evidentiary purposes according to standard procedures until the law enforcement authorities request them.

Training:

- Where applicable and appropriate, the policy and guidelines will be incorporated into training and orientation programs of Bluewater Employees, volunteers and service provider(s). Training programs addressing obligations under the Act shall be conducted as necessary.