

CORPORATE POLICY AND PROCEDURE



POLICY	Video Surveillance Policy
CATEGORY	Corporate
AUTHORITY	City Clerk's Office
RELATED POLICIES	Access and Privacy Policy, Records and Information Management (RIM) Policy
APPROVED BY	Executive Team
EFFECTIVE DATE	March 23, 2017

POLICY STATEMENT

The City of Guelph recognizes the delicate balance between an individual's right to be free from invasion of privacy and the need to protect the safety and security of its employees, the public and property. In respecting this balance, the City is committed to ensuring and enhancing the safety and security of the public, its employees and property by integrating security best practices with the responsible use of technology. Employees ensure the personal information of persons captured on video surveillance is maintained as private, confidential and secure, except as legally exempted or in situations outlined by this policy.

PURPOSE

The objectives of video surveillance systems are to enhance the safety and security of employees, the public and corporate assets, to prevent unauthorized activities on or involving City property and reduce risk and liability exposures.

SCOPE

This policy applies to all City of Guelph employees, including full-time, part-time, casual, contract, volunteer and co-op placement employees.

Contractors and service providers are afforded the same rights and expectations as employees in this policy, while performing authorized activities for the City.

This policy applies to all video surveillance systems located in all City properties and facilities.

This policy does not apply to covert surveillance used as an investigation tool for law enforcement purposes or in contemplation of litigation.

POLICY

The City of Guelph is responsible for the video surveillance systems and maintaining custody and control of video records at all times.

The collection of personal information through video surveillance is authorized under section 28(2) of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

Providing notice

Signs are posted at all public access points to and within areas under video surveillance.

All attempts are made to ensure proper signage is posted at all facilities using a video surveillance system.

Camera placement

Where possible, all cameras that are adjustable or moveable are restricted to prohibit the viewing of locations not intended to be monitored. Cameras are prevented from looking through a window of an adjacent building or areas where a higher level of privacy is expected, such as within a washroom or change room.

Only the Manager Bylaw Compliance, Security and Licensing in coordination with the City Clerk or delegated employees, may install, change or authorize a service provider or employee to install or **change a camera's permanent setting**.

Use of video recordings

The information collected through video surveillance is used only for the purposes of:

- Enhancing the safety and security of employees, the public and corporate assets;
- Preventing unauthorized activities upon or involving City property;
- Assisting in investigating unlawful activity;
- Assessing the effectiveness of safety and security measures;
- Investigating an incident involving the safety or security of people, facilities or assets;
- Providing **evidence as required to protect the City's legal rights**;
- Investigating an incident or allegation of serious employee misconduct;
- Managing corporate risk;
- Investigating an incident involving a potential or active insurable claim; or
- A consistent purpose.

Any time an incident report is completed, applicable video will be pulled and retained as needed.

When a City employee is involved in an incident for which a video recording is being pulled, that video recording must be reviewed and pulled by another employee or manager.

Requests for disclosure

The City of Guelph does not disclose a video record to any individual or organization except as permitted through MFIPPA.

1. Public requests for disclosure - Any person may make a written request for access to video records created through a video surveillance system through the freedom of information process. Access 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.
2. Internal requests for disclosure – City employees or consultants may request a copy of a video recording if it is necessary for the performance of their **duties in the discharge of the institution's functions.**
3. Law enforcement requests - The City may disclose a copy of a video recording to a law enforcement agency where there are reasonable grounds to believe that an unlawful activity has occurred and been captured by the video surveillance system in accordance with section 32.(g) of MFIPPA.

If video containing personal information is improperly disclosed or is suspected to have been disclosed to an unauthorized person, the employee or service provider who is aware of the disclosure must immediately inform the appropriate department manager, as well as, the City Clerk or delegated employees.

Live viewing

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, or the commission of unauthorized activity in the area under surveillance. Live feed monitors are turned off when not in use.

Retention and destruction

Video that has not been requested by the public, City employees or law enforcement agencies within the maximum retention period is considered transitory and is automatically erased by being overwritten in accordance with the records retention by-law.

Certain City facilities use digital video recording equipment to store information until the storage capacity of the hard drive/video tape has been reached at which time the image is overwritten. All new installed or upgraded digital video recording

equipment in City facilities are programmed with a maximum retention period of five (5) calendar days after which time it is overwritten.

If video is proactively pulled in anticipation of a request, video may be stored for up to thirty (30) calendar days. If no request is received within the thirty (30) days then it is manually deleted.

Digital recording equipment may only be destroyed when replaced by a new piece of equipment or when it is not repairable. It may only be destroyed by an authorized service person and it is destroyed in a manner that ensures that it can no longer be used by any person and that the information recorded cannot be reconstructed or retrieved by any person.

RESPONSIBILITY

The Chief Administration Officer (CAO) will:

- Provide oversight and compliance with this policy by all City employees.

Deputy Chief Administration Officers (DCAO's) will:

- Administer and communicate this policy broadly to all employees in their service areas.

The City Clerk and delegated employees will:

- Respond to requests for disclosure under the freedom of information or applicable routine disclosure procedures;
- Ensure a public notice for video surveillance is placed at all City sites that have a video surveillance system;
- Respond to requests from the public and employees about the collection, use, and disclosure of personal information captured by a video surveillance system;
- Respond to appeals and privacy complaints received through the Office of the Information and Privacy Commissioner of Ontario (IPC);
- Educate employees and visitors on the collection, use, and disclosure of personal information through the video surveillance system;
- Work with department manager(s) and employee(s) in the event of an improper disclosure of personal information;
- Notify the IPC in the event of a privacy breach, where appropriate;
- Conduct internal audits of the system, as required, to ensure compliance with this policy and MFIPPA.

General managers, managers and supervisors will:

- Ensure the appropriate use of the video surveillance system at their facility(ies) in compliance with this policy;
- Delegate and assign responsibility regarding who will act on their behalf in following procedures relating to this policy in their absence;
- Provide job-specific training;
- Refer any requests for copies of surveillance video to the City Clerk or delegated employees;
- Investigate and report any privacy breaches to the City Clerk or delegated employees;
- Ensure that employees are monitoring compliance with the retention periods applicable to the video surveillance systems.

Employees will:

- Report to their manager or supervisor any suspected privacy breach;
- Report to their supervisor any problems with the video surveillance system;
- Review and comply with this policy and MFIPPA in performing their duties and functions related to the operation of the video surveillance system.

Employees may be subject to criminal charges, civil liability and/or discipline, including but not limited to termination, for a breach of this policy, or provisions of MFIPPA or other relevant statutes.

MONITORING AND EVALUATION

The City Clerk's Office monitors compliance, engagement and awareness of this policy with:

- access to information reporting documents under the routine disclosure and freedom of information processes;
- the results of audits;
- training and education session evaluations; and
- employee surveys.

This policy is reviewed a minimum of once per calendar year to ensure its effectiveness and compliance with legislation and current business processes or as required based on legislative changes.

For further information regarding this policy please contact the Program Manager Information, Privacy and Elections at 519-822-1260 extension 2605 or at privacy@guelph.ca.

REFERENCE MATERIAL

Municipal Freedom of Information and Protection of Privacy Act

http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm

Personal Health Information and Protection Act

http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm

Information and Privacy Commissioner

<http://www.ipc.on.ca/english/Privacy/>

APPENDIX A: DEFINITIONS

City means the Corporation of the City of Guelph.

Clerk means the City Clerk of the Corporation of the City of Guelph.

Consistent purpose means personal information collected by the City of Guelph is used for the purpose for which it was collected or similar consistent purposes when carrying out City business. The individual to whom the information relates might reasonably expect the use/disclosure of their personal information for those consistent purposes.

Control (of a record) means the power or authority to make a decision about the use or 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 is the physical or electronic disposal of records or data by means of shredding, recycling, deletion or overwriting. This also includes the destruction of records or data residing on computers and electronic devices supplied or paid for by the Corporation.

Digital video recording equipment means any type of video recording and reception equipment used as part of the video surveillance system.

Freedom of information process means a formal request for access to records made under the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

Head refers to the City Clerk.

Information and Privacy Commissioner means the Information and Privacy Commissioner of Ontario (commonly referred to as the IPC). The IPC hears appeals of decisions made by Heads of institutions, issues binding orders, conducts privacy investigations, and has certain powers relating to the protection of personal privacy as set out in the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) means legislation that governs access to and the privacy of municipal records.

Personal information 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 the financial transactions in which the individual has been involved;
 - c) Any identifying number, symbol, or other particular 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
 - h) **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 stolen, lost or accessed by unauthorized persons.

Record means any unit of information however recorded, whether in printed form, on film, by electronic means, or otherwise, and includes correspondence, memoranda, plans, maps, drawings, graphic works, photographs, film, microfilm, sound recordings, videotapes, machine readable records, an e-mail and any other documentary material regardless of physical form or characteristics, made or received in the course of the conduct of City business.

Retention period is the period of time during which a specific records series must be kept before records in that records series may be disposed of.

Service provider means a video service provider, consultant or other contractor engaged by the City in respect of the video surveillance system.

Video surveillance system means a video, 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 public spaces or within City operated facilities.