POLICY TITLE: VIDEO SURVEILLANCE

POLICY NUMBER: CORP-2020-

DATE:

POLICY STATEMENT

The Town of Halton Hills recognizes the 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 Town 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 Town properties and Town facilities and reduce risk and liability exposures.

SCOPE

This policy applies to all employees whose duties include requesting, installing, accessing and monitoring video surveillance equipment and video footage at all Town properties and in all Town facilities. Contractors and service providers are afforded the same expectations as employees in this policy, while performing authorized activities for the Town.

This policy applies to all video surveillance systems located on all Town properties and in all Town facilities. It may, when applicable, apply to other digital equipment used for Town business.

This policy does not apply to audio taping of Council and Committee meetings or theatre productions.

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

POLICY

The Town of Halton Hills is responsible for the video surveillance systems and maintaining custody or control of digital 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 to be posted at public access points and within areas under video surveillance. (SCHEDULE 2)

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

Audio

Many new systems offer the ability to record audio, however, this feature should not be used as doing so may constitute “wiretapping” in violation of the Criminal Code of Canada.

If audio is a standard feature on any video surveillance system used by the Town it must be disengaged.

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 Commissioner of the relevant site, in coordination with the Clerk & Director of Legislative Services 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 Town 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 Town’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 submitted, applicable video may be pulled and retained as needed.

When a Town employee is involved in an incident, for which a video recording is being pulled, that video recording must be reviewed and pulled by the facility supervisor or, if the incident pertains to a facility supervisor, it must be reviewed and pulled by another facility supervisor or the Manager or Commissioner of that facility.

Requests for Disclosure

The Town of Halton Hills does not disclose a video record to any individual or organization except as permitted through MFIPPA.

1. Law Enforcement

   The Town 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.

   The Law Enforcement Agency must submit their request for access to video surveillance **in writing** via email, correspondence or in person to the Facility Supervisor or Manager unless there are reasonable and probable grounds to believe that the circumstances pose an immediate threat to the health or safety of an individual or others.

   The **Video Surveillance Record Request – Authorized Release or Access or Access Denied** form must be completed by the Supervisor or Manager or Commissioner of the facility. (SCHEDULE 1)

2. Internal Request

   Town employees may request the Supervisor, Manager or Commissioner of a facility to investigate an incident using video surveillance records.

3. Municipal Investigation or Claim Against the Municipality

   In a municipal investigation or claim against the municipality, the Town employee or representative must submit their request for access to video surveillance **in writing** via email, correspondence or in person to the Facility Supervisor.

   The **Video Surveillance Record Request – Authorized Release or Access or Access Denied** form must be completed by the Supervisor, Manager or Commissioner of the facility. (SCHEDULE 1) A copy of the completed form should be forwarded to the Clerk & Director of Legislative Services.

4. Registered Town Facility Users, specifically Community Organizations, may have occasion to request access to video surveillance records of the Town in support of an incident investigation conducted by the organization or a governing body into the conduct of one or more members of their organization. Any registered Town Facility Users, specifically Community Organizations, may make a written request for access to video surveillance records through

the Freedom of Information process. Consideration will be given to the prudent use of video footage in any investigation particularly if the use is in support of the objectives of any Town policy (e.g., Zero Tolerance policy).

If the matter becomes a law enforcement investigation, access to the video may be provided to the law enforcement agency upon request. (Refer to 1. Law Enforcement).

5. Member(s) of the Public – Any person may make a written request for access to video surveillance records 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.

   If the matter becomes a law enforcement investigation, access to the video may be provided to the law enforcement agency upon request. (Refer to 1. Law Enforcement)

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 Supervisor of the facility, who will immediately advise their Commissioner and the Clerk & Director of Legislative Services or delegated employees.

Retention and Destruction

Video that has not been requisitioned for use in an investigation (MFIPPA or other) within the maximum retention period is considered transitory and is erased by being overwritten in accordance with the retention schedule.

Certain Town-owned digital video recording equipment stores information until the storage capacity of the hard drive/videotape has been reached at which time the image is overwritten. On the date this policy takes effect, any current Town-owned digital video recording equipment that can be programmed with a maximum retention period of **ten (10)** calendar days will be programmed as such; after which time it will be overwritten. In future, all new installed or upgraded digital video recording equipment on Town property will be programmed with a maximum retention period of **ten (10)** calendar days after which time it will be overwritten.

If video is proactively pulled in anticipation of an access request, video may be stored for up to **ninety (90)** calendar days. If no request is received within the **ninety (90)** days it is to be deleted. An exception will be for video pulled for a reported personal injury. It may be stored for up to **2 years**. If no request is received within the **2 year period** it is to be deleted.

Surplus digital video recording equipment 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 Town employees.

Senior Management Team will:

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

The Clerk & Director of Legislative Services, the Information Governance and Records Management Specialist and delegated employees will:

- Respond to requests for disclosure under the Freedom of Information process or applicable routine disclosure procedures.
- Ensure a public notice for video surveillance is placed at all Town 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.

Commissioners, 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.
- Investigate and report any privacy breaches to the Clerk & Director of Legislative Services or delegated employees.
- Ensure that employees are monitoring compliance with the retention periods applicable to the video surveillance systems.

Employees will:

- Consult with Information Technology Services on impacts for any new or modified video surveillance system installation.
- 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 Clerk & Director of Legislative Services and Information Governance and Records Management Specialist will monitor 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 and employee surveys; and
- training and education session evaluations.

This policy is reviewed a minimum of once every two calendar years 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 Information Governance and Records Management Specialist at 905-873-2600 extension 2356

DEFINITIONS

Consistent purpose(s) means personal information collected by the Town of Halton Hills is used for the purpose for which it was collected or similar consistent purposes when carrying out Town 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).

Information and Privacy Commissioner means the Information and Privacy Commissioner of Ontario (commonly referred to as the IPC). The IPC receives appeals for 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 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 Town 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 Town with respect to the video surveillance system(s).

Town means the Corporation of the Town of Halton Hills.

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 and on all Town properties and in all Town facilities.

SCHEDULE 1 (Side 1)

VIDEO SURVEILLANCE RECORD REQUEST
AUTHORIZED RELEASE or ACCESS or ACCESS DENIED

Requester Name	
Request Type	☐ FOI #: ☐ Investigation #: ☐ Claim (e.g., Insurance) File # ☐ Subpoena/Warrant/ Court Order #:
Incident Details	

Camera Location	Facility No.
Date on Footage	
Start Time on Footage	
End Time on Footage	
Reviewed by	
Date of Review	
Option 1 APPROVAL for	☐ RELEASE Device? (usb/dvd/other):
Option 2 APPROVAL for	☐ ACCESS to View ONLY at Town Office Location: Date: Time:
Option 3 DENIED	Reason:
Approved/Denied by	

The video surveillance record, identified as: _____
is RELEASED **or** ACCESSED with the understanding it will not be duplicated or released online and will be used only for the express purpose for which it was requested and in accordance with Section 32(g) of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and Town Policy **CORP-2020-XXXX**.

Received by ☐ Viewed by ☐

Name (PLEASE PRINT) **Institution / Organization Name** **Badge # (if applicable)**

Signature **Date**

SCHEDULE 1 (Side 2)

VIDEO SURVEILLANCE RECORD REQUEST
AUTHORIZED RELEASE or ACCESS or ACCESS DENIED

This form must be completed for the release of or access to video surveillance footage or when access to video surveillance footage is denied.

LAW ENFORCEMENT

Law Enforcement agencies frequently require access to records containing personal information from municipalities. The disclosure of records containing personal information is restricted under Part II of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). Section 32(g) of the Act permits the disclosure of personal information by an institution (e.g., Town of Halton Hills) to a law enforcement agency in Canada for the purpose of aiding an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

Law enforcement officer(s) will need to cite the legislative reference under which they have authority to receive the information and must submit their law enforcement institution name, badge number; and investigation number.

Law Enforcement agencies include but are not limited to Police Services, Workplace Safety & Insurance Board, Employment Insurance, Welfare and Social Insurance agencies, Social Assistance, Ministry of Revenue (Income Tax), Property Standards, Municipal Law Enforcement, Conservation Authorities, etc. If unsure, the agency should provide the section of the Act that gives them the authority to access such records.

Law Enforcement agencies must submit their request for access to video surveillance **in writing** via email, correspondence or in person to the Facility Supervisor or Manager, unless there are reasonable and probable grounds to believe that the circumstances pose an immediate threat to the health or safety of an individual or others.

MUNICIPAL INVESTIGATION or CLAIMS AGAINST THE MUNICIPALITY

In a municipal investigation or claim against the municipality, the Town employee or representative must submit their request for access to video surveillance **in writing** via email, correspondence or in person to the Facility Supervisor.

REGISTERED TOWN FACILITY USERS or MEMBER(S) OF THE PUBLIC

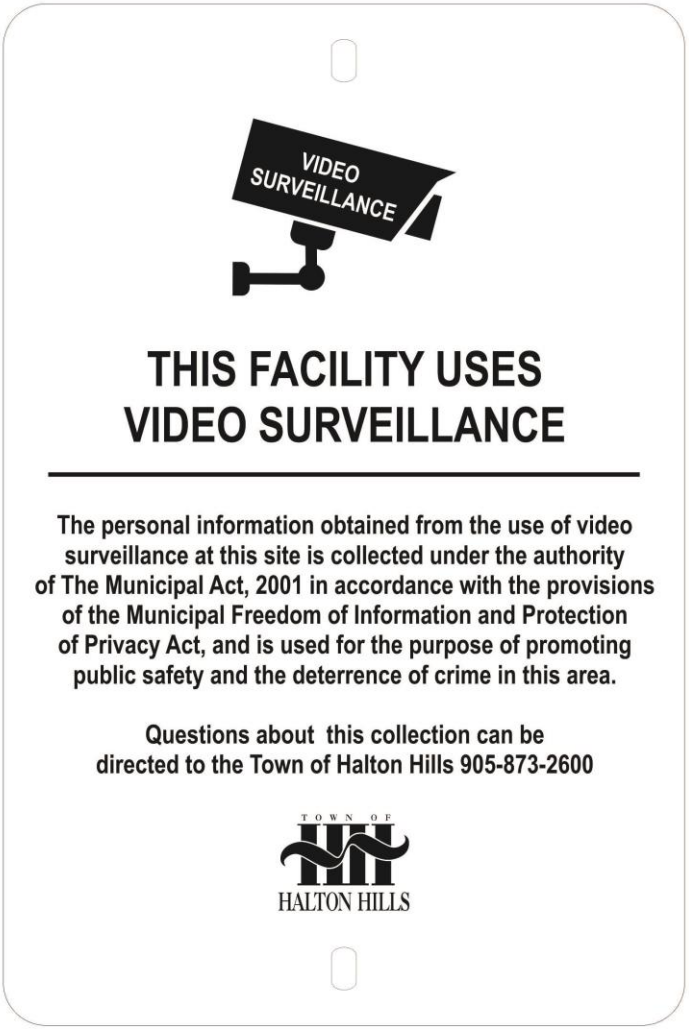
All non-law enforcement requesters must submit their request for access to video surveillance through the Freedom of Information process.

Contact the Information Governance and Records Management Specialist at 905-873-2600 extension 2356.

Complete the other side and forward a copy to the Clerk & Director of Legislative Services

SCHEDULE 2

VIDEO SURVEILLANCE SIGNAGE



VIDEO SURVEILLANCE DECALS