FORTFRANCES
BOUNDLESS

VIDEO SURVEILLANCE

ADMINISTRATION & FINANCE 1.22

POLICY

Created: 2023-06-12

Revised:

Authorized: 2023-06-12

Superseded:

1. PURPOSE

(1) The Town is committed to the goal of a safe and secure workplace. The Town's Video Surveillance Program compliments other measures taken by the Town to:

(a) Promote the safety of customers, staff, and the community; and

(b) Protect Town assets and property against theft or vandalism.

(2) The Town is also dedicated to fostering community safety and well-being. In partnership with the OPP, the Town's Video Surveillance Program is used for law enforcement purposes within the jurisdiction of the Town and the OPP, and is intended to:

(a) Deter criminal and quasi-criminal activity;

(b) Enhance and support OPP investigations; and

(c) Increase court convictions by providing evidence of criminal or quasi-criminal activity.

(3) This policy establishes controls for the Town's Video Surveillance Program by governing the use of Video Surveillance Systems and Video Surveillance Records owned or operated by the Town by:

(a) Directing the operation of Recording Devices on Town property and in public spaces;

(b) Identifying the responsibilities of Users accessing Video Surveillance Systems and Video Surveillance Records; and

(c) Informing the community about the Town's Video Surveillance Program.

2. APPLICATION

(1) This policy applies to all Users who:

(a) Create, distribute, access, or manage Video Surveillance Records owned by the Town; and

(b) Access or manage Video Surveillance Systems owned or operated by the Town.

(2) This policy does not apply to meetings taking place through audio or video conferencing.

3. USER RESPONSIBILITIES

3.1. ROLES

(1) The Chief Administrative Officer is responsible for the Video Surveillance Program.

(2) The Municipal Clerk is responsible for:

(a) The Video Surveillance Program's compliance with MFIPPA; and

(b) Responding to requests for access to Video Surveillance Records in accordance with MFIPPA.

(3) The Manager of each Division is responsible for:

(a) Authorizing the installation of Recording Devices in any physical locations under their supervision;

(b) Documenting the rationale for the installation of Recording Devices in any physical locations under their supervision; and

(c) Sufficiently funding the installation and maintenance of any Video Surveillance Systems that they have authorized.

(4) The Manager of each Department is responsible for:

(a) Establishing operating procedures that specify the circumstances in which access to Video Surveillance Systems and Video Surveillance Records will be required by Users under their supervision;

(b) Identifying the Users under their supervision to be authorized by the IT Department to access Video Surveillance Systems and Video Surveillance Records;

(c) Ensuring Users under their supervision comply with the Video Surveillance Policy;

(d) Directing any investigations of reported incidents that require the review of Video Surveillance Records collected from any physical locations under their supervision; and

(e) Maintaining records of all instances of access to and use of Video Surveillance Records by Users under their supervision.

(5) The Information Technology Manager is responsible for:

(a) The life-cycle management of any Video Surveillance Systems, including but not limited to:

(i) Specifying required equipment and operating parameters; and

(ii) Installation and maintenance of hardware and software;

(b) Maintaining records of:

(i) Where Recording Devices are installed;

(ii) When Recording Devices are in operation;

(iii) The authorization and rationale for monitoring each location; and

(iv) The Users authorized to access Video Surveillance Systems and Video Surveillance Records;

(c) Posting a ***Notice of Collection of Personal Information*** in monitored areas.

(d) Training authorized Users to operate Video Surveillance Clients; and

(e) Ensuring Video Surveillance Systems can only be accessed by authorized Users.

(6) The OPP is responsible for:

(a) Adhering to the Memorandum of Agreement between the Town and the OPP regarding the use of and access to the Town's Video Surveillance Systems.

3.2. COMPLIANCE

(1) Users shall comply with all Town policies, procedures, and standards while using Video Surveillance Systems and Video Surveillance Records, including but not limited to:

(a) The ***Information Technology Resources Policy*** (3.20).

(2) Users shall comply with the laws and regulations of all applicable jurisdictions while using Video Surveillance Systems and Video Surveillance 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 Code***; and

(e) MFIPPA.

(3) Users shall comply with any audit or investigation by the Town surrounding their use of Video Surveillance Systems and Video Surveillance Records.

3.3. ACCEPTABLE USE

(1) Video Surveillance Systems may be used to:

(a) Monitor Recording Devices in real-time;

(b) Review Video Surveillance Records; and

(c) Extract and archive Video Surveillance Records.

(2) Recording Devices shall be monitored in real-time only for the purposes intended by the Town, including but not limited to:

(a) System maintenance carried out by the IT Department;

(b) Active incident response; and

(c) Viewing areas that require real-time monitoring, as prescribed by established operating procedures.

(3) Video Surveillance Records shall be reviewed, extracted, or archived only for the purposes intended by the Town, including but not limited to:

(a) System maintenance carried out by the IT Department;

(b) Investigation of reported incidents; and

(c) Viewing events in areas that require recordkeeping, as prescribed by established operating procedures.

(4) Incidents shall be investigated only for the purposes intended by the Town, including but not limited to:

(a) The protection of Town property;

(b) The protection of customers, staff, and the community; and

(c) The detection and deterrence of theft, vandalism, and other criminal or quasi-criminal activity.

(5) Logs shall be kept of all instances of access to and use of Video Surveillance Records.

(6) Users shall take every precaution reasonable to protect against unauthorized access to Video Surveillance Records.

(7) Use of Video Surveillance Systems and Video Surveillance Records is subject to audit.

(8) Agreements with service providers or other parties shall explicitly state that Records dealt with or created during the working relationship and under the Town's control and are subject to MFIPPA.

4. SECURITY

(1) The Town shall always maintain control of its Video Surveillance Systems.

(2) Recording Servers shall operate in strictly controlled areas accessible only by the IT Department.

(3) Access to Video Surveillance Clients shall be restricted to authorized Users.

5. RECORDING DEVICES

(1) Recording Devices shall be placed overtly and labelled as Town equipment.

(2) Recording Devices shall be installed only where they are expected to be the most effective to support law enforcement efforts and operating procedures, including:

(a) Areas of Town facilities identified as requiring monitoring, including but not limited to:

(i) The Civic Centre and Fire Hall;

(ii) The Museum;

(iii) The Memorial Sports Centre;

(iv) The Public Library Technology Centre;

(v) The Public Works Office and Yard;

(vi) The Airport; and

(vii) The Water Treatment Plant; and

(b) Public areas identified by the Safe Streets Program, including:

(i) The Millennium Park;

(ii) The Rainy Lake Square;

(iii) The Front Street Marina;

(iv) The alley between First Street and Scott Street (from Mowat Avenue to Victoria Avenue);

(v) Scott Street (from Central Avenue to Armit Avenue);

(vi) The alley between Scott Street and Church Street (from Mowat Avenue to Victoria Avenue);

(vii) Church Street (from Mowat Avenue to Armit Avenue); and

(viii) Portage Avenue (from First Street East to Nelson Street).

(3) Recording Devices may produce Video Surveillance Records continuously, with exceptions in operation arising from limited system capabilities, service disruptions, and maintenance.

(4) Remotely adjustable Recording Devices shall not be manipulated to monitor areas that are not intended to be monitored by the Town.

(5) Recording Devices shall be regularly inspected to ensure their operation complies with this policy.

6. COLLECTION OF PERSONAL INFORMATION

(1) The Town's collection of Personal Information as Video Surveillance Records through its Video Surveillance Systems is lawfully authorized through this Video Surveillance Policy which has been adopted through a by-law and is intended to explicitly protect:

(a) The public assets of the municipality;

(b) Economic, social, and environmental well-being of the municipality;

(c) Health, safety, and well-being of persons;

(d) Services and things that the municipality is authorized to provide;

(e) Persons and property, including consumer protection; and

(f) Structures including fences and signs.

(2) A ***Notice of Collection of Personal Information*** shall be made by way of signage.

(3) Signage shall be in place that provides the community reasonable and adequate warning about the use of Recording Devices by:

(a) Being clearly written;

(b) Being prominently displayed at pedestrian entrances and the interior walls of buildings where Recording Devices are installed; and

(c) Being prominently displayed at pedestrian entrances to public spaces where Recording Devices are installed.

(4) Signage shall satisfy notification requirements under Section 29(2) of MFIPPA by:

(a) Describing the legal authority for the collection of personal information;

(b) Describing the principal purpose for which the personal information is intended to be used; and

(c) Directing questions about the collection of personal information to the Town's Municipal Clerk by including their title, business address, and telephone number.

7. RETENTION AND DISPOSAL OF VIDEO SURVEILLANCE RECORDS

(1) Video Surveillance Records produced from Recording Devices that have not been extracted as part of an investigation shall be overwritten at the end of their retention period, being:

(a) A minimum of 7 days; and

(b) A maximum of 28 days.

(2) Video Surveillance 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) A minimum of 1 year.

8. PRIVACY

(1) Video Surveillance Systems shall not be configured to collect audio Records.

(2) Recording Devices shall not monitor areas where customers, staff and the community have a higher expectation of privacy, including but not limited to:

(a) The interior of washrooms, showers, and change rooms.

(3) Recording Devices shall not monitor residential areas that are not generally observable by the community from a public space.

(4) 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:

(a) Windows and doors.

(5) Digital masks shall obscure Video Surveillance Records in a manner that is removable only by authorized Users.

9. TRANSPARENCY

(1) The Town shall endeavour to be as transparent as possible about the operation of its Video Surveillance Systems without compromising the security of those systems.

(2) The Town shall make the following information available to the community through the Town's website, and upon request through other accessible formats as well:

(a) The rationale for video surveillance;

(b) The objectives of video surveillance; and

(c) The ***Video Surveillance Policy***.

(3) Video Surveillance Records are subject to relevant legislation and may be accessed by requests through MFIPPA.

10. REVIEW

(1) This policy shall be reviewed by Town Council no later than one year after its implementation.

(2) This policy shall be reviewed by Town Council at least once per term of Council.

11. DEFINITIONS

- **"Authorization"** means approval explicitly obtained from the IT Department, including but not limited to:
    - Configurations of permissions to IT Resources granted by the IT Department in consultation with a User's supervisor; and
    - Written requests for permissions from a User's supervisor to the IT Department.
- **"Department"** means a small organizational unit of the Town.
- **"Division"** means a large organizational unit of the Town that contains Departments.
- **"IT"** means Information Technology.
- **"IT Department"** means the Town's IT Manager and any staff under the direction of the Town's IT Manager.
- **"MFIPPA"** means the ***Municipal Freedom of Information and Protection of Privacy Act*** of Ontario.
- **"OPP"** means the Ontario Provincial Police – Rainy River District (Northwest Region).
- **"Personal Information"** as defined in section 2 of MFIPPA means:
    - "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. Therefore, a simple image on a video surveillance system that is clear enough to identify a person, or the activities in which he or she is engaged in, will be classified as personal information under the Act."
- **"Record"** as defined in section 2 of MFIPPA means:
    - "Any information, however recorded, whether in printed form, on film, by electronic means or otherwise, and includes: a photograph, a film, a microfilm, a microfiche, a videotape, a machine-readable record, and any record that is capable of being produced from a machine-readable record."
- **"Recording Device"** means any analog or digital device used to produce Records that can be collected by a Video Surveillance System, including but not limited to:

  - Video cameras;
  - Infrared cameras; and
  - Microphones.

- **"Recording Server"** means any device that collects Video Surveillance Records from a Recording Device.
- **"Safe Streets Program"** means a community public safety initiative that expands the Town's Video Surveillance Program into public spaces of downtown Fort Frances.
- **"Town"** means the Corporation of the Town of Fort Frances.
- **"User"** means any individual that accesses Video Surveillance Systems or Video Surveillance Records, including but not limited to:
  - Town staff and volunteers;
  - Contractors; and
  - OPP staff.
- **"Video Surveillance Client"** means any software application that enables observation or production of Video Surveillance Records from a Recording Device.
- **"Video Surveillance Program"** means the policies and procedures authorizing the use of Video Surveillance Systems by the Town, including the Safe Streets Program.
- **"Video Surveillance Record"** means any Record produced from a Recording Device.
- **"Video Surveillance System"** means a collection of hardware and software components that enables centralized recording, observation, and archiving of Video Surveillance Records, including but not limited to:
  - Video Surveillance Clients;
  - Recording Devices; and
  - Recording Servers.