



# qathet

## REGIONAL DISTRICT

<b>SECTION 1</b>	<b>CORPORATE POLICIES</b>
<b>POLICY</b>	<b>1.19</b>
<b>SUBJECT</b>	<b>VIDEO SURVEILLANCE POLICY</b>
<b>ADOPTED</b>	<b>MARCH 06, 2024</b>

---

### 1. POLICY STATEMENT

- 1.1 Section 30 of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires that a public body protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized collection, use, disclosure or disposal. Section 26 of FOIPPA identifies the purposes for which personal information may be collected. Because video surveillance systems create a record that may contain personal information, a public body should implement security policies and procedures.
- 1.2 Video surveillance systems will only be used by qathet Regional District (qRD) in, on, or near facilities owned or occupied by qRD and used for public civic purposes when necessary to ensure the safety and protection of individuals and/or qRD property and assets, or to perform functions designed to carry out all or part of a qRD mandate.

### 2. DEFINITIONS

“**CAO**” means the Chief Administrative Officer for the qRD, or his or her delegate.

“**Corporate Officer**” means the Corporate Officer for the qRD, or his or her delegate.

“**contact information**” means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.

“**department manager**” means the manager of the qRD department responsible for the operation of the video surveillance system, or his or her delegate.

“**FOIPPA**” means the *Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165*.

**“personal information”** means recorded information about an identifiable individual other than contact information.

**“PIA”** means a privacy impact assessment, which identifies and mitigates the risks to personal information arising from the implementation of new projects and assists with compliance to FOIPPA.

**“record”** means any information recorded by a video surveillance system.

**“video surveillance system”** refers to any mechanical, electronic or digital system or device owned or operated by or for qRD that: (i) enables continuous or periodic video recording, observing or monitoring of individuals, assets and/or property; and (ii) is intended to be mounted or affixed to a structure, fixture or vehicle. For greater certainty, "video surveillance system" does not include cell phones with video capability, hand-held video recorders or video conferencing systems.

### **3. PURPOSE**

- 3.1 To establish guidelines for the use of video surveillance systems owned or operated by or for qRD that enhance the security and safety of persons, properties, assets, and activities that are in, on, or near facilities owned or occupied by qRD and used for public civic purposes.
- 3.2 To ensure that all video surveillance systems owned or operated by or for qRD appropriately respect privacy and are compliant with FOIPPA.

### **4. SCOPE**

- 4.1 This policy applies to all video surveillance systems owned or operated by or for qRD.
- 4.2 This policy does not apply to video or audio recordings of qRD meetings, including but not limited to Board or Committee meetings, public engagement sessions and public hearings.
- 4.3 This policy does not apply to video surveillance conducted by the Royal Canadian Mounted Police (RCMP), who are subject to the *Privacy Act* (Canada).
- 4.4 This policy does not extend to private property, as video surveillance systems will only be used in, on, or near facilities owned or occupied by qRD and used for public civic purposes.

## **5. GUIDELINES**

### **Authority to Install and Operate a Video Surveillance System**

- 5.1 The CAO must grant approval for the installation of a video surveillance system and for any substantial material change proposed to the use or purpose of an existing video surveillance system.
- 5.2 A PIA is required for all video surveillance system installations, whether or not they collect personal information, and when making a material change in use or purpose of an existing video surveillance system. A PIA will be prepared by a department manager and approved by the Corporate Officer, and will include:
  - a) the rationale and purpose of the video surveillance system;
  - b) the location and field of vision of the equipment;
  - c) the type and location of the notification to the public that the public will be under video surveillance;
  - d) rationale and purpose of the specific locations of equipment and fields of vision selected;
  - e) times when surveillance will be in effect;
  - f) whether or when recording will take place; and
  - g) the purpose for which a record will be accessed.
- 5.3 If the video surveillance system no longer meets the criteria in clause 1.2 of this policy, the video surveillance system must be disabled and removed.
- 5.4 The department manager is responsible for ensuring that any third party service provider engaged to work on a video surveillance system, or to supply video surveillance services under contract for qRD, is bonded, made aware of this policy and applicable procedures, and agrees in writing to be bound by them. Breach of this policy by a third party service provided may lead to penalties up to and including contract termination.

### **Video Surveillance System Audits**

- 5.5 The Corporate Officer, with the support of the Technical Services Department, will conduct audits of qRD video surveillance systems randomly on an annual basis in order to confirm compliance with FOIPPA and adherence to this policy and the associated procedures. The results of each review should be documented in detail and any concerns should be addressed promptly and effectively. The Corporate Officer may require that a video surveillance system be disabled and removed if it is non-compliant with FOIPPA, if it no longer adheres to this policy and the associated procedures, or if it is no longer necessary to fulfill its intended purpose as identified in the original or any revised PIA.

## **Video Surveillance System Restrictions**

- 5.6 Video surveillance systems must not be used to verify staff attendance or to monitor staff performance.
- 5.7 Video surveillance must not take place in areas considered confidential or normally private, e.g. changing rooms and washrooms.
- 5.8 Cameras must be installed in such a way that they only monitor those areas that have been identified in the PIA as requiring video surveillance.
- 5.9 Adjustment of camera positions and field of view must be restricted, if possible, to ensure only those areas that have been identified in the PIA as requiring video monitoring are being monitored.
- 5.10 Video surveillance must be restricted to those time periods when the system is serving its intended purpose, as set out in the PIA.
- 5.11 Sound should not be recorded unless there is a specific need to do so and doing so complies with the *Criminal Code* (R.S.C., 1985, c. C-46).

## **Video Surveillance System Security, Access and Logs**

- 5.12 Physical and electronic security must be in place to ensure the protection of video surveillance systems and records.
- 5.13 All individuals who have access to video surveillance systems must undergo privacy training to understand their obligations under FOIPPA.
- 5.14 A video surveillance system operations log must be created by the department manager showing the dates and times of operation, the location and field of view of the video surveillance cameras, and the position titles of those that have access to the surveillance system. Changes to any of these factors must be logged.
- 5.15 The department manager must identify, in the PIA, the position titles in each location that are authorized to access the video surveillance system and the video surveillance system operations log.

## **Retention and Destruction of Video Surveillance Records**

- 5.16 All video surveillance records must be retained for a period of no longer than 14 days and destroyed at the end of this retention period, unless:
  - a) the record reveals an incident that contains personal information about an individual and qRD uses this information to make a decision that directly affects the individual, in which case the video surveillance records must be retained for one year after the decision is made so that the affected individual has reasonable opportunity to obtain access to the personal information;

- b) the department manager requires the video surveillance records to be preserved for an additional period of time in order to complete the business purpose for which the video surveillance records were created. In such a case, the department manager must make a written request to the Corporate Officer, setting out the basis on which an extension is required. Upon receipt of the request, the Corporate Officer may decline or grant the request for an extension to a fixed date; or
- c) a request is made to the Corporate Officer for longer retention as a result of contemplated or current litigation.

### **Video Surveillance System Records Access and Disclosure**

- 5.17 Access to video surveillance records is to be for the purpose set out in the PIA.
- 5.18 The department manager, CAO, Corporate Officer or Manager of Technical Services must be present if video surveillance records are being accessed or viewed.
- 5.19 A log must be created and maintained by the department manager to record all instances of personal information being viewed in a video surveillance record, the purpose of the viewing, date and time of the viewing, and the identities of those present during the viewing, the location of the recording camera(s) and the start and end times viewed in the record.
- 5.20 Video surveillance records may be used by qRD as evidence in any civil proceedings.
- 5.21 Disclosure requests must be made in writing to the Corporate Officer. Only the Corporate Officer may authorize disclosure of video surveillance records. In order to enable a proper audit trail, logs must be kept of any such instance of disclosure.
- 5.22 Other than disclosure to law enforcement, or use for qRD purposes in accordance with this policy, video surveillance records will only be released on the authority of a production order to seize the record for evidence or other court order.
- 5.23 Information recorded by video surveillance may be released to law enforcement only by the Corporate Officer with the use of a law enforcement release form which includes a statement of assurance that the disclosed information will be confidentially destroyed when it is no longer required for the purpose for which it was disclosed.
- 5.24 For shared facilities, qRD may share video surveillance system records with third parties that participate in the operation of the facility, with prior approval of the Corporate Officer, where a disclosure of personal information is in

accordance with FOIPPA. A written information sharing agreement must be in place between the qRD and the third party before video surveillance records will be shared.

## **Transparency**

5.25 As a general rule, FOIPPA requires qRD to notify individuals when their personal information may be collected.

5.26 Individuals must be notified of the existence and use of video surveillance systems (functional or non-functional) through qRD branded signage that is clearly written and prominently displayed at the entrance of all locations where a video surveillance system is in operation. The sign will include an image of a video camera.

5.27 Signs must indicate which area is under video surveillance and for what purpose and must include the office address and phone number for the Corporate Officer. For example, a sign may say:

*“To ensure a safe and respectful environment for patrons and staff, and to prevent loss of property, video surveillance is in use at various locations on this site. Images are collected in accordance with, and subject to, the provisions of the Freedom of Information and Protection of Privacy Act. Questions – contact the Corporate Officer at qathet Regional District at 202–4675 Marine Avenue or 604-485-2260”.*

## **Process for Handling Complaints of Breach of this Policy**

5.28 Complaints about a breach of this policy will be handled in accordance with qRD’s General Complaints Policy 2.11.

## **6. RESPONSIBILITY / AUTHORITY TO ACT**

6.1 The Corporate Officer will oversee and administer the policy and has responsibility overall for all of the qRD video surveillance systems and records.

6.2 The CAO is responsible for granting approval for the installation of a video surveillance system and for any substantial material change proposed to the use or purpose of an existing video surveillance system.

6.3 Department managers will ensure that qRD’s video surveillance systems are operated in accordance with this policy and the associated procedures.

6.4 The Technical Services Department will oversee the lifecycle management of qRD’s video surveillance systems including, but not limited to design, installation, maintenance, physical and electronic security, replacement and disposal.

6.5 qRD staff will comply with this policy and related acts. Breach of this policy or of any procedure created pursuant to it by an employee may result in discipline up to and including discharge.

## **7. POLICY REVIEW DATE**

7.1 This policy will be reviewed periodically.

## **8. RELATED POLICIES OR ACTS**

- 2.11 General Complaints Policy
- *Freedom of Information and Protection of Privacy Act*