

DISTRICT OF FORT ST. JAMES

POLICY AND PROCEDURE MANUAL

POLICY GROUP:	Building & Property
POLICY#:	3.12
SUBJECT:	Surveillance Policy
ADOPTED:	April 27, 2016 (Resolution No. 2016-08-22)
REVISED:	
ADMINISTERED BY:	Administration

POLICY

The District of Fort St. James respects personal privacy and only collects personal information that relates directly to and is necessary for an operating program, or for the purposes of law enforcement. Video surveillance is conducted in accordance with the Freedom of Information and Protection of Privacy Act.

PURPOSE

To establish guidelines for the use of video surveillance to enhance the security and safety of persons, properties, things, and activities that are in, on, or near facilities owned or occupied by the District of Fort St. James and used for public or civic purposes.

SCOPE

This Policy applies to any video surveillance system operated by or for the District of Fort St. James that collects personal information in the form of recorded images of individuals.

PROCEDURES

Principles

- As an owner of public assets that represent an investment of public money, the District of Fort St. James wishes to make use of video surveillance systems to better protect the security of its people, assets and property.
- The District acknowledges that the use of video surveillance may, in some circumstances, represent an intrusion into personal privacy; the District does not wish to impair personal privacy any more than is warranted to provide necessary and reasonable protection of its property against vandalism, theft, damage and destruction.
- The District has the right to investigate activity of a criminal nature on its property.
- Video surveillance recordings may be used by the District for the investigation of and as evidence in any civil proceedings.

- Video surveillance must only be in public places and must be practically minimized.
- Surveillance will not take place in areas considered confidential or normally private, e.g. change rooms, washrooms.
- Video surveillance is not to be used to supervise staff performance or to verify staff attendance in the workplace.

Designated Responsibilities

- The Chief Administrative Officer is responsible for the overall video surveillance program. Each Department Head is responsible for ensuring that procedures, as established in this policy, for the use of video surveillance equipment, including the random audit of such procedures, are in accordance with this policy.
- The Public Works Superintendent is responsible for the life cycle management of authorized video surveillance systems including, but not limited to, specifications, installation, maintenance, replacement, disposal, and related requirements, including signage.
- District employees and service providers shall review and comply with the policy in performing their duties and functions related to the operation of video surveillance systems. District employees may be subject to discipline if they knowingly or deliberately breach the policy.

Video Surveillance Requirements and Use

- Before implementing a surveillance system or expanding an existing video surveillance system, the reason for introducing or expanding the video surveillance is to be clearly articulated in writing, and approval for the introduction or expansion of video surveillance must be granted by the Chief Administrative Officer.
- The need for video surveillance must clearly meet the criteria of this Policy and the installation must conform to this Policy and be approved by the Chief Administrative Officer. The Chief Administrative Officer, when considering a proposal, will consider the following:
 - a) Incident reports respecting vandalism, theft, property damage, and safety concerns.
 - b) Safety or security measures in place currently or attempted before installing video surveillance.
 - c) Safety or security problems that video surveillance is expected to resolve.
 - d) Areas and/or times of operation.
 - e) Expected impact on personal privacy.
 - f) How the video surveillance will benefit the District or is related to District business.

- g) How the benefits are expected to outweigh any privacy rights as a result of video surveillance.
- h) How it will protect the security and safety of persons.

Use, Access, and Security

- Access to video surveillance information is limited to the following individuals:
 - a) Security Contractor (e.g. Marina Manager)
 - b) Chief Administrative Officer
 - c) Department Heads
 - d) District Solicitor
 - e) RCMP members, in order to access data necessary to investigate a law enforcement matter.
- Use of video surveillance information is to be for the purposes of investigation of an incident in any public place. Information Technology staff will access the equipment only for the purpose of maintaining, backing up the software, and assisting with the extraction of the portions of the data. District staff may be authorized to view, retrieve and access video surveillance for a specific purpose.
- Physical and computer related security must be in place at all times to properly secure access to the recording equipment and video data. Detailed logs that record all instances of access to and use of the recording equipment and video material must be maintained at all times by the relevant department.
- Records of video surveillance systems that collect personal information must be protected in accordance with the Freedom of Information and Protection of Privacy Act.
- The locations and times of all video material must be maintained in logs and kept current by the relevant department. Generally, the video surveillance equipment or screen must be located so that the public is not able to see any video reproduction.
- Video surveillance data or videotapes may not be publicly viewed or distributed in any fashion. Video data must not be altered in any manner, with the exception of saving investigation material related to an incident on public places or information required for law enforcement purposes. Other than release to the RCMP, or use for District of Fort St. James purposes in accordance with this Policy, video surveillance data will only be released on the authority of a warrant to seize the recorded data for evidence or other court order.
- Any other requests for access to incident specific information must be referred to the Chief Administrative Officer and will only be disclosed in accordance with the FOIPPA.

Retention and Destruction

- The District will use a recording system that overwrites data on a continual basis. Retention of the recorded video data is determined by the amount of available space within the District's storage facilities and the type of medium used to store such data.
- Recorded data that has been saved to another medium, for investigation purposes, will be retained for at least one year after being used, so that the affected individual has a reasonable opportunity to obtain access to that personal information. Such recorded data is to be destroyed after one year or after the affected individual has had access to the data, unless otherwise required for legal, administrative or other proceedings.
- Old storage devices must be securely disposed of based on media format by shredding, burning or magnetic erasure.

Signage

- It is a requirement of the Freedom of Information and Protection of Privacy Act that individuals be notified when the District collects their personal information. Accordingly, at each facility where video surveillance takes place, signs not less than 30 cm x 30 cm in size must be prominently displayed at entrances to and egresses from the facilities.
- The sign must clearly state the following:
"This area is monitored by video surveillance cameras. For further information contact the Chief Administrative Officer. 250-996-8233."
- A pictogram of a video camera (such as the one shown to the right) must also be shown on the sign.



Training

- When applicable and appropriate, the policy and guidelines will be incorporated into training and orientation programs of the corporation.
- Training programs addressing staff involvement with the use and monitoring of video surveillance equipment under the policy and under the Freedom of Information and Protection of Privacy Act shall be conducted as required.