Video Surveillance System
Policy 218, 2025

The following was adopted as Policy by Resolution No. 2025-0X-xxx at the Regular Council Meeting held on Month, day, **2025.**

PURPOSE

Where the District of Lake Country ("District") determines the use of **Video Surveillance System**s are required to protect the safety, protection or security of people, assets, property or for law enforcement purposes, this Policy establishes standards for the implementation, use, access, disclosure, retention and destruction of **Video Surveillance System**s and their **Footage**.

POLICY

1. DEFINITIONS

Footage means any video, audio, images, or any other **Personal Information** collected through **Video Surveillance System**s.

Personal Information recorded information about an individual including, home address, phone number, email, SIN, gender, age, birthdate, personal opinions, license plate number, personal characteristics, health and medical information, financial and employment information, other sensitive information that could be used to identify a specific person. **Personal Information** is not business contact information which includes business name, position or title, business telephone, address or email.

Privacy Head means the District staff appointed as the Head of the privacy management program or their designate, in accordance with British Columbia's *Freedom of Information and Protection of Privacy Act* (*FOIPPA*).

Privacy Impact Assessment (PIA) means an assessment conducted by the District to identify, assess, and mitigate privacy risks and determine if a current or proposed initiative, system, project, program, or activity meets the requirements of *FOIPPA*.

Private Location means an area wherein a person would have a reasonable expectation not to be observed or monitored by **Video Surveillance System**s, including but not limited to locations such as changing rooms, bathrooms, and private office rooms.

Public Location means a common area where privacy should not be expected, and where observing or monitoring a person through **Video Surveillance System**s does not violate that person's privacy. Such locations may include but are not limited to parks, public spaces, parking lots, garages, elevators, building entrances, and walkways.

Video Surveillance System means a surveillance system that is capable of recording video, audio, images, or any other **Personal Information**, either continuously or periodically, in real-time or stored, and which may be used to observe or monitor individuals, assets, or property.

2. SCOPE

2.1. This Policy applies to all **Video Surveillance Systems** owned, managed, and maintained by the District. This Policy is not applicable to traffic cameras, cameras or video of Committee or Council meetings, video surveillance conducted by the Royal Canadian Mounted Police ("RCMP") or cameras operated by a third-party.

2.2. The **Privacy Head** is responsible for administering this Policy and any standards and operational procedures developed to support this Policy.

3. THIRD PARTY VIDEO SURVELLIANCE AT DISTRICT FACILITIES

3.1. Lease or license agreements for the use of District-owned land or facilities must include a clause requiring third parties to comply with the *Personal Information Protection Act (PIPA)* if a Video Surveillance System is installed.

3.2. Third parties must provide written notice of a Video Surveillance System to the District at least 30 days prior to installation, including:

(a) purpose of the surveillance
(b) confirmation that less privacy-invasive options were considered
(c) a release and indemnification of the District from privacy breaches or complaints
(d) acknowledgement of privacy obligations and compliance with *PIPA*
(e) details on public signage to be installed, if any

4. INSTALLATION

4.1. **The installation of Video Surveillance System**s must be approved by the **Privacy Head** and Information Management Department.

4.2. Prior to submitting a proposal for **Video Surveillance System** installation, staff should explore alternative methods of deterring unwanted activity that may be less invasive to privacy.

4.3. If it is determined that there are no better alternatives, a request to install a **Video Surveillance System** may be submitted to the **Privacy Head** outlining the following:

(a) the purpose and rationale for the system.
(b) areas and time of operations
(c) issues it would address
(d) benefit versus the risk to privacy rights
(e) the proposed location
(f) reports on vandalism, theft, property damage, liability, and safety concerns in the area
(g) any pre-existing security measures that are already in place

4.4. Prior to installation of an approved **Video Surveillance System** or expanding an existing system, a **PIA** will be conducted to assess how privacy rights will be affected.

5. LOCATIONS

5.1. **Video Surveillance Systems** will not be installed in **Private Locations**.

5.2. **Video Surveillance Systems** may only be installed in **Public Locations** if the installation is determined to be necessary for the safety, protection or security of people, assets, property or for law enforcement purposes.

5.3. External monitors or screens of **Video Surveillance System**s must be positioned to ensure recorded or live **Footage** is not visible to the public, unless the **Privacy Head** has specifically approved the public display for the purpose of deterring criminal or inappropriate behaviour.

5.4. **Video Surveillance Systems** should be located:

(a) in a location that collects the minimum amount of personal information necessary to achieve the purpose
(b) in a location that is most effective in meeting the purpose of the surveillance
(c) in a position that does not monitor other buildings or look through windows of adjacent buildings
(d) if used for surveillance related to crime, be restricted to the time periods when there is demonstrably higher likelihood of crime

6. NOTICE OF SURVEILLANCE

6.1. In accordance with *FOIPPA* section 27(2), the District will post highly visible signage that notifies the public the area is under surveillance and include District contact information for inquiries.

6.2. Information regarding how and when **Footage** is captured will be set out in the **PIA** conducted prior to the installation of a **Video Surveillance System**.

7. COLLECTION AND SECURITY OF FOOTAGE

7.1. **Video Surveillance System Footage** is the property of the District.

7.2. Only permitted Staff may collect, access, use, and disclose **Footage**.

7.3. Operation of a **Video Surveillance System** must be conducted professionally, ethically, and consistent with applicable District policies, and any federal or provincial legislation or regulations.

7.4. The Information Management Department is responsible for:

(a) establishing equipment specifications standards for the installation, maintenance, replacement and equipment disposal in accordance with District policy
(b) physical and electronic security measures to safeguard the **Footage**
(c) destruction of **Footage** after 15 days and no later than 60 days, except for where required for legal matters
(d) training authorized staff on the technical use of a **Video Surveillance System**
(e) retaining a list of locations of **Video Surveillance System**s cameras

7.5. The **Privacy Head** is responsible for:

(a) ensuring **Personal Information** collected through a **Video Surveillance System** is protected, used or disclosed under the provisions of *FOIPPA*

(b) ensuring users of a **Video Surveillance System** are aware of the legislative and policy privacy obligations

(c) providing guidance on best practices regarding the retention and destruction of **Footage**

8. ACCESS, USE, AND DISCLOSURE OF FOOTAGE

8.1. Access and use of **Footage** is limited to the Chief Administrative Officer (CAO), the **Privacy Head**, staff designated by the **Privacy Head**, the Director of Legal Services and Risk Management, the Information Manager and RCMP in relation to a law enforcement matter.

8.2. Access, review, and disclose of **Footage** will be done in compliance with bylaws, and applicable federal and provincial legislation.

8.3. **Footage** will not be used to surveil or supervise performance of District staff unless it is determined by the **CAO** and **Privacy Head** to be appropriate based on a significant need for security, health, and safety purposes.

8.4. **Footage** may be disclosed for the purposes of aiding in a law enforcement investigation or for purposes related to imminent health or safety concerns. Where requested for law enforcement purposes, staff will obtain a case file number from the authorized body prior to release.

8.5. **Footage** may only be disclosed through secured sharing means approved by the Information Management Department and must follow that department's set protocols to ensure the **Footage** being shared remains protected.

8.6. Once video **Footage** is disclosed to an authorized recipient, custody and responsibility for that **Footage** transfers to the recipient. The District is not responsible for the **Footage** after its release.

8.7. Requests for specific **Footage** by third parties must be made through the District's Freedom of Information Request process. When permitted to be released in accordance with *FOIPPA* and impractical to sever **Personal Information** from the **Footage**, the District may release stills taken of the **Footage**, with appropriate severing applied.

8.8. Any individual who is subject of surveillance has the right to request access to their recorded **Personal Information** under section 5 of *FOIPPA*. Release of **Footage** may require the identity of other individuals in the **Footage** to be blurred or otherwise concealed.

8.9. The Information Management department may access the **Video Surveillance System**s for maintenance, back-ups, extractions of **Footage** as needed, and any other technological support as may be required to ensure the **Video Surveillance System**s are functional.

9. RETENTION AND DESTRUCTION OF FOOTAGE

9.1. **Footage** may be destroyed at any time after 15 days and must be destroyed promptly after 60 days have passed, except if the District is required to retain the **Footage** for legal matters.

9.2. **Footage** must be securely disposed of based on media type and may include erasure, overwriting, magnetic erasure or shredding.

9.3. When **Footage** has been disclosed in response to a Freedom of Information Request, for investigative purposes, for legal matters or for internal purposes, the District will retain **Footage** for at least one year.

10. AUDITS

10.1. **Video Surveillance System**s will be internally audited on an ongoing and as needed basis by the **Privacy Head** and Information Management Department to ensure that these systems remain functional.

11. CONSEQUENSES

11.1. Any access, collection, use, or disclosure of **Footage** for purposes other than those set out in this Policy are prohibited.

11.2. If **Video Surveillance System**s are installed without following the processes set out in this Policy, they will be turned off until a **PIA** has been completed, and the **Privacy Head** and Information Management department has approved its use in accordance with this Policy.

12. APPROVALS, AMENDMENTS AND ANNUAL REVIEWS

Date	Approver	Type

Paul Gipps, Chief Administrative Officer

Date