Maple Ridge

COUNCIL POLICY

Title: CCTV (Video Surveillance) Policy		**Policy No:** 30.15 **Supersedes:** 30.15 (Dec. 19, 2017)
Effective Date: December 19, 2017	**Amended Date:** November 12, 2024	**Review Date:** November 12, 2026

Policy Statement:
The City has installed video surveillance systems at City facilities to keep the City's facilities, its staff, and the community of Maple Ridge secure.

Purpose:
The purpose of this Policy is to set standards for the implementation, use, access, and disclosure of video surveillance systems at City Facilities.

Scope:
This Policy applies to all City Staff and all video surveillance cameras owned, managed, and maintained by the City.

This Policy is not applicable to:

- traffic cameras; and
- cameras used temporarily for City events, Committee meetings, or Council meetings.

Definitions:
Any key terms for the City are set out in Schedule A of the Policy Governance Framework and may be relied on as if they were a part of this Policy. If there is any discrepancy between the definitions in this Policy and the Framework, this Policy's definitions will prevail.

CCTV means closed circuit television cameras.

CCTV Staff means any City Staff designated by the Privacy Head that access, review, and disclose Footage from the City's Video Surveillance Systems, as permitted by City policies, bylaws, and federal and provincial legislation.

City Staff means any person employed by the City or any person who has been assigned or hired to act on the City's behalf.

FOIPPA means British Columbia's *Freedom of Information and Protection of Privacy Act*, RSBC 1996 c 165, as amended from time to time, which governs the protection of privacy and Personal Information held in the custody or control of local public bodies, including the City.

Footage means any video, audio, images, or any other Personal Information that is collected through Video Surveillance Systems.

Personal Information means recorded information about an identifiable individual, other than business contact information.

Privacy Head means the City Staff member appointed as the Head of the privacy management program at the City, or their designate, in accordance with British Columbia's *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165.

Privacy Impact Assessment (PIA) means an assessment that is conducted by the City to determine if a current or proposed enactment, system, project, program, or activity meets or will meet the requirements of FOIPPA, as defined under FOIPPA. It is also conducted to identify, assess, and mitigate privacy risks, ensure compliance with FOIPPA and foster trust and accountability in the handling of personal information.

Private Location means an area wherein a person would have a reasonable expectation to not be observed or monitored by Video Surveillance Systems, 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 Systems does not violate that person's privacy. Such locations may include but are not limited to 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. Such systems include but are not limited to CCTV.

Procedure:

<u>Installation</u>

1. ***Installation Proposal***
    a. Prior to submitting a proposal for Video Surveillance System installation, City Staff should explore potential alternative methods of deterring unwanted activity that may be less invasive to privacy.

b. If it is determined that there are no better alternatives, then a request proposing the installation of a Video Surveillance System may be submitted to the Privacy Head.

c. The following factors will be considered in a proposal for the installation of a Video Surveillance System:

i. the purpose for the installation of the Video Surveillance System, the issues that it would address, and the benefit of this versus the risk it may have to privacy rights;
ii. the proposed location of the Video Surveillance System;
iii. reports on vandalism, theft, property damage, liability, and safety concerns in the area; and
iv. any pre-existing security measures that are already in place.

d. Video Surveillance Systems may not be installed at City facilities unless the submitted proposal is approved by the Privacy Head.

e. A Privacy Impact Assessment will be conducted by the City's Privacy Head for the proposed installation of any new Video Surveillance Systems prior to their installation to assess how privacy rights will be affected.

2. *Locations*

a. Video Surveillance Systems may only be installed in Public Locations if:

i. approval in writing for the installation has been granted by the Privacy Head, and
ii. the installation is determined to be necessary due to imminent safety concerns or for law enforcement purposes.

b. Video Surveillance Systems, including any external screens that display information related to those Video Surveillance Systems, must be situated in such a way to prevent Footage from being publicly visible, unless such display is approved by the Privacy Head for the purposes of deterring criminal or otherwise unwanted behaviour.

3. *Notice of Surveillance*

a. The City will post highly visible signage that notifies the public that the area is under surveillance and provide City contact information for inquiries.

b. 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.

Footage

4. *Collection and Security of Footage*

a. Video Surveillance System Footage is the property of the City.

b. Only permitted CCTV Staff may collect, access, use, and disclose Footage, and any operation of the Video Surveillance Systems must be conducted in such a way that is professional, ethical, and consistent with applicable City policies, and any federal or provincial legislation or regulations.

c. Physical and electronic security measures will be implemented by the Information Technology department and the Privacy Head to safeguard the Footage that is recorded and stored on the Video Surveillance Systems.

i. A list of CCTV Staff and the locations of the Video Surveillance Systems cameras will be kept by the Privacy Head in an appropriate records repository to ensure that access to these systems is safeguarded.

d. The Privacy Head will ensure that Personal Information collected through these systems is protected and only used or disclosed under the provisions of FOIPPA.

5. *Access, Use, and Disclosure of Footage*

a. Access and use of Footage by City Staff will be done in compliance with the Privacy Management Program Policy and any applicable legislation.

b. Footage will not be used to surveil City Staff unless it is determined by the Privacy Head to be appropriate based on a significant need for security, health, and safety purposes.

c. When the City discloses Footage to an authorized recipient, the Disclosed Footage will be deemed to be in the custody of the recipient and the City will no longer be responsible for the Disclosed Footage once it is released.

d. Requests for specific Footage for any other purpose by third parties must be made through the City's Freedom of Information Request process and in accordance with the provisions of FOIPPA. The City may release stills taken of the footage, with appropriate severing applied, when it is impractical to sever the personal information of others from the video footage.

e. IT and service technicians may access the Video Surveillance Systems for the purposes of providing maintenance, back-ups, extractions of Footage as needed, and any other technological support as may be required to ensure the Video Surveillance Systems are functional.

f. Footage may be disclosed for the purposes of aiding in a law enforcement investigation or for purposes related to imminent health or safety concerns.

i. CCTV Staff will confirm that the request for Footage is for law enforcement purposes. A case file number being provided from an authorized body is sufficient confirmation for this purpose.

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

h. For the purposes of tracking disclosure, the Privacy Head will keep a copy of any Footage that is provided to a third party or used internally for a purpose consistent with this policy.

i. If any concerns are reported regarding the access and disclosure of Footage, these concerns will be addressed through the Privacy Management Program Policy.

6. *Retention and Destruction of Footage*

a. Footage in the Video Surveillance System must be retained for a minimum of 30 days but may not be retained for more than 60 days. The Privacy Head may provide guidance on best practices regarding the retention and destruction of Footage in the Video Surveillance System.

b. Footage may be destroyed after 30 days have passed. Any Footage held past the 30-day minimum may be destroyed at any time, and if held for up to 60 days, must be destroyed promptly after 60 days have passed. An exception to these retention dates will be made if the City must retain the Footage for extenuating circumstances as indicated in the Records Management Policy, such as:

i. for the production of documents related to litigation matters and for any documents that are under a legal hold, or
ii. retaining copies of any disclosed Footage and evidence of authorization for the disclosure of the Footage.

c. Notwithstanding the retention and destruction periods set out in section 6, when Footage is disclosed for any of the purposes set out in 6(b)(i) and 6(b)(ii), the Footage must be retained by the City for at least one year.

7. *Training*

a. CCTV Staff will receive ongoing and as needed training by IT and the Privacy Head on the technical use of the Video Surveillance Systems once they become authorized to access these systems, and on the privacy obligations they must adhere to in accordance with legislative and policy requirements.

8. *Audits*

a. Video Surveillance Systems will be internally audited on an ongoing and as needed basis by the Privacy Head and IT department to ensure that these systems remain functional.

Administration:

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

Consequences:

10. Any access, collection, use, or disclosure of Footage for purposes other than those set out in this Policy are prohibited. Any violations of such may result in disciplinary action under the City's Human Resources policies.

11. If Video Surveillance Systems are installed without following the processes set out in this Policy, they will be turned off until a PIA has been completed by the Privacy Head and the Privacy Head has approved its use in accordance with this Policy.

(Administration Only) **Resolution No.:**	**Signature** _____	**Date Signed** _____