

Procedure Information	
Related to Policy No:	AD-FA-3.12
Approved by:	Executive Committee
Approval Date:	September 28, 2022
Executive Responsible	Vice President Finance & Corporate Services
Administrator Responsible:	Director, Safety & Security
Date of Next Review:	September 2024

VIDEO SURVEILLANCE OF PUBLIC AREAS PROCEDURES

Definitions

Disclosure

The act of sharing, displaying, or otherwise providing personal information to a third party.

Personal Information

Recorded information about an identifiable individual other than business contact information, as defined in the BC Freedom of Information and Protection of Privacy Act (FIPPA). Personal information may be collected in any visual medium (photography, video, etc.) and in any format (WMV, JPEG, JVI, HTML, etc.)

Surveillance system

Any video surveillance technology (such as video cameras, closed circuit television cameras, still-frame cameras, digital cameras, and time-lapse) that enables continuous or periodic viewing or monitoring. Audio recordings are not captured by the surveillance system.

Procedures

1. Management of the System

1.1. The Director, Safety & Security is responsible for the management and operation of the College of New Caledonia ("CNC" or "the College") surveillance system. This includes:

- 1.1.1. oversight to ensure that the system's day-to-day use complies with College policies, as well as FIPPA;
- 1.1.2. training for all authorized personnel;
- 1.1.3. the security of all recorded or collected information;
- 1.1.4. the release of, or access to, any recorded information; and
- 1.1.5. periodic audits of the system.

2. Public Awareness of Surveillance Systems

2.1. Signage will be posted to notify the public when they are entering a zone which is monitored by video surveillance equipment.

2.2. Signage will be clearly visible and will direct viewers to a URL where they can access the following information:

- 2.2.1. the purpose for the collection of surveillance recordings;
- 2.2.2. the intended use for the recordings; and
- 2.2.3. the person(s) to contact if they have any questions.

3. Authorized Personnel

3.1. The Director, Safety & Security is responsible for granting access to the surveillance system's recorded video and images. Personnel authorized to regularly access surveillance system footage include:

- 3.1.1. Security Services staff; and
- 3.1.2. Regional Campus Principals and Operations Managers.

3.2. All personnel who are authorized to operate surveillance systems and access surveillance footage will receive regular training related to video surveillance and privacy.

4. Use of Surveillance System Footage

- 4.1. Authorized personnel will have access to live and recorded images from the surveillance installations and may monitor images actively for the purpose of maintaining safety on campus.
- 4.2. Authorized personnel are not permitted to use the surveillance system to view residential or private areas, or to monitor individuals in any manner that would be an unreasonable invasion of privacy. Surveillance recordings are subject to audit procedures and personnel may be required to justify their actions.
- 4.3. Authorized personnel, upon observing suspicious activity, may isolate the camera, and if available, can use the pan, tilt, and zoom features to determine if a response is required.
- 4.4. If Security Services personnel determine a response is required, the personnel should use the surveillance system to identify the involved parties for evidence purposes. This may include the surveillance of a person from one area to another.
- 4.5. Security Service personnel will record all incidents in the incident reporting system and include all pertinent information.

5. Ownership of Information

5.1. Ownership of the recorded material, in whatever medium, remains the property of the College.

6. Retention and Disposal of Surveillance System Recordings

6.1. Security Services will keep logs of all use, disclosure, and destruction of surveillance system recordings.

- 6.2. Surveillance system data is retained for no more than 30 days, with the following exceptions:
- 6.2.1. if it is needed to facilitate or document an investigation or legal proceeding, the recording may be retained for as long as required for that purpose; and
 - 6.2.2. if it has been used to make a decision that directly affects an individual, the recording must be retained for at least one year after the date of that decision.
- 6.3. When retained recordings are no longer required, they must be securely destroyed.

7. Access to and Disclosure of Recorded Information

- 7.1. Access to recorded information is only permitted in accordance with this policy and with FIPPA. Material may not under any circumstances be sold or used for commercial purposes or for the provision of entertainment.
- 7.2. Access to recorded information is restricted to:
- 7.2.1. authorized personnel as outlined in Section 3;
 - 7.2.2. those responsible for the administration of the College surveillance system;
 - 7.2.3. individuals seeking images or recordings in which they themselves appear (as outlined in subsection 7.4.); and
 - 7.2.4. law enforcement agencies granted access to recorded images to assist in a specific investigation.
- 7.3. Requests for surveillance system recordings must be approved by the Director, Safety & Security prior to disclosure of surveillance system images or recordings.
- 7.4. Individuals whose image or likeness is captured by surveillance technologies have the right to access a copy of the relevant recording(s), subject to:
- 7.4.1. the submission of a written request providing enough detail to enable, within a reasonable effort, the identification and isolation of the recording(s) in question;
 - 7.4.2. written proof of consent granted to an authority to apply, and otherwise act, on the individuals' behalf if necessary and/or requested;
 - 7.4.3. the use of masking technologies to ensure that all identifying information of other individuals who may be present on the recording(s) is not disclosed; and
 - 7.4.4. all other applicable legislation, including FIPPA.

7.5. All disclosures of surveillance system recordings must be logged as incidents in the College's incident reporting system, supported by the following information:

- 7.5.1. the date and time at which access was approved or the date on which disclosure was made;
- 7.5.2. the date and time the recording or images were captured;
- 7.5.3. the credentials of the person who was allowed access or to whom disclosure was made; and
- 7.5.4. the reason for allowing access or disclosure.

8. Auditing & Oversight

8.1. The Director, Safety & Security will periodically audit the video surveillance system, including monitors and storage systems, to determine whether any changes need to be made in the use or configuration of the systems.

Other Related Policies, Documents, and Websites

Video Surveillance of Public Areas AD-FA-3.12

Freedom of Information and Protection of Privacy Act

Public Sector Surveillance Guidelines

Procedure Amendment Log

Amendment Number:	Date:
0	September 28, 2022
1	
2	