KWANTLEN POLYTECHNIC UNIVERSITY

Policy History
Policy No. SR13
Approving Jurisdiction: President
Administrative Responsibility: Vice President Finance and Administration
Effective Date: February 5, 2018

Closed Circuit Video Equipment (CCVE) Procedure

A. DEFINITIONS

1. **CCVE:** Closed Circuit Video Equipment.
2. **CSO:** Chief Safety Officer.
3. **CSS:** Campus Safety and Security.
4. **Safety/Security Event:** An event on a University campus involving the safety or security of persons or University property.
5. **The *FIPPA*:** The *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165
6. **The Policy:** Policy SR13 Closed Circuit Video Equipment (CCVE) Policy.
7. **Recording:** Video image recorded and stored by the CCVE system.
8. **University:** Kwantlen Polytechnic University.

B. PROCEDURES

1. Responsibilities

a. The CSO oversees the management of the CCVE system operations and will ensure the day to day compliance with the requirements of the Policy and the *FIPPA*.

b. The CSO or authorized designate will approve access to, use of and disclosure of recordings collected by the CCVE system.

c. The CSO may not delegate his/her responsibilities under section 1(a), but may by written delegation appoint an authorized designate to exercise his/her responsibilities under section 1(b).

2. Operation

a. The CCVE system monitors identified locations, including exterior pathways, walkways and building entrance, egress points, parking lots, student enrolment services front counters. The CCVE system cameras operate 24 hours a day, 7 days a week.

b. Operation and access by identified individuals to the CCVE system must be approved in writing by the CSO or authorized designate.

c. In an emergency, and where it is not reasonably practical to secure prior written

authorization from the CSO or authorized designate, the duty Security Supervisor may grant access to persons whose job or responsibilities require access to the CCVE system.

d. The CSO will conduct quarterly compliance audits to ensure that all access to and use of the CCVE system complies with the terms of this Procedure, the Policy and the FIPPA.

e. A log recording all persons entering the CCVE monitoring area (including name, date, time and reason for attending) shall be kept in the Security Room.

3. Notification

a. The CSS will ensure that signs providing notice of the CCVE equipment will be posted at all locations where cameras are active.

b. Notices will be clearly visible.

4. Collection, Use, Disclosure, Retention, and Destruction of Recordings

a. Recordings collected by the CCVE system will not be routinely monitored or reviewed on a continuous basis.

b. Real-time monitoring will only occur when authorized by the CSO or authorized designate. Real time monitoring of the CCVE system may occur: during an active Safety/Security Event (e.g. intrusion system activates, emergency on campus) that has been reported to the CSS; or, as otherwise permitted or required by law.

c. Access to Recordings must be approved in writing by the CSO or authorized designate. Such access may be granted in response to a Safety/Security Event or as permitted or required by law.

d. The CCVE system will be used in compliance with the University's Policy HR15 Diversity & Inclusiveness.

e. The CCVE System is protected by reasonable technological, organizational, and physical security measures, including storage of all Recordings in a secure location and measures to prevent unauthorized access, tampering, loss, theft and unauthorized duplication of Recordings.

f. Recordings will usually be destroyed 30 days after creation, unless otherwise permitted or required by law or unless the footage is required for other purposes. All recordings will be securely destroyed when no longer needed. Recorded data that has been saved to another medium, for investigation or evidentiary purposes, will be retained for at least one year after being used, or as otherwise permitted or required for legal, administrative or other purposes.

g. Requests for access to Recordings will be processed as permitted or required by law. The University may, at its discretion, redact or provide opportunities to view footage rather than releasing copies of Recordings.

5. Locations

a. Specific locations of the CCVE cameras will be chosen to meet the purposes and objectives of the CCVE system as set out in the Policy. All locations with active cameras will have posted notices clearly visible to the public advising of the use of

surveillance, its purposes, the legal authority for its use, and including contact information for a University official who may be contacted with queries about the CCVE system.

b. CCVE cameras will be clearly visible to the public, and will not be directed to areas in which there is a usual expectation of privacy (e.g. residences or washrooms).

c. Once cameras are installed, the field of view of may only be adjusted with the permission of the Chief Safety Officer.

d. The CCVE system shall not be used for monitoring employees for the purposes of tracking productivity or performance evaluation.

C. RELATED POLICIES

Refer to SR13 *Closed Circuit Video Equipment (CCVE) Policy*.