G1004 – VIDEO SURVEILLANCE

PROCEDURES

1. Requests for Disclosure

The procedure for dealing with requests made under section 3.5 of the policy for disclosure of video footage or still images gathered by the Langara College Video Surveillance System is as follows:

a. The person will forward a request in writing to the Manager, Records Management and Privacy (the Manager). This request must include the precise location of the camera, the date and approximate time of the suspected surveillance, a photograph or description of the person making the request and a mailing address for the person making the request.

b. Within three (3) days of receipt of the request, the Manager will inspect the digital files to determine if the camera in question recorded video at the specified time.

c. If video was recorded by the camera at the specified time, the Manager will review the recording to determine if the person making the request appears in the recording.

d. If the person making the request appears in the recording, a copy of the recording will be made. All video frames showing persons other than the person making the request, and all frames that do not show the person making the request, will be removed. The copy of the video file showing only the person making the request will be saved in DVD format and mailed to him or her.

If surveillance video is not provided to a requester for any reason, the Manager will provide that person with an explanation in writing within 30 business days. The College will not provide surveillance video to a requesting party if:

- The required information is not provided in the original request.
- The camera in question did not record video at the time specified.
- The recorded information has been automatically over-written because data storage has reached its capacity.
- The person making the request does not appear in the recording.
- Other persons appear in each video frame in which the requester also appears, and the College is unable to protect the privacy of the other persons by masking, pixilation or other means.

2. Register of Video Surveillance Cameras

The Register of Video Surveillance Cameras will specify the:

a. precise location of each camera,

b. nature of each camera, including technical specifications such as resolution, frame rate, colour or grey scale, low light capability, and pan/tilt/zoom (PTZ) function,

c. area under observation by each camera,

d. specific purpose for each camera (e.g. deter and detect unauthorized entry through the northeast main floor A building door).

3. Record Keeping

Video Surveillance Activity Log:

A Detailed Video Surveillance Activity Log of all surveillance activities will record:

a. Video surveillance detecting activity resulting in a response by Campus Security;
b. Video surveillance video being retained for investigative purposes;
c. Video surveillance being used to make a legal or administrative decision in respect to a person;
d. Video surveillance video being provided to a law enforcement officer;
e. Video surveillance video being provided to individuals under surveillance;
f. Video surveillance video being provided to third parties;
g. Law enforcement officers being denied video surveillance video for any reason;
h. Individuals under surveillance being denied video surveillance video for any reason;
i. Third parties being denied video surveillance video for any reason;
j. Written direction or authorization relating to any of the above; and
k. All other relevant information about each incident in question including, in the case of video or still pictures being retained for one year or more, a copy of the video or still pictures.

The Video Surveillance Activity Log will be held in a safe and secure location with the video surveillance equipment. All authorized persons with access to the video surveillance images will have access to the log and are responsible for entering their own log data at the time of the activity. This log will be audited annually by the Manager, Safety, Security and Emergency Management.

4. Retention, Storage and Access

a. All video or digital recordings maintained by authorized personnel will be automatically over-written when data storage has reached its capacity unless they are retained as part of a criminal investigation, pending court proceedings (criminal or civil) or other bona fide use as approved by the Director, Facilities.

b. The Manager, Safety, Security and Emergency Management will retain recordings that contain personal information about an individual, and are used to make a decision that directly affects the individual, for one year after the decision is made pursuant to section 31 of the B.C. Freedom of Information and Protection of Privacy Act. Recordings used for evidence in any criminal or civil proceedings will be retained by the Manager, Safety, Security and Emergency Management until any subsequent appeal periods have expired.

c. Video surveillance equipment, controllers, storage devices and data will be stored in a secure on-site location with limited access by authorized personnel only.

d. All storage devices that are not in use shall be stored securely in a locked area located in a controlled access area.

e. Access to the data on storage devices is limited to authorized personnel who will be trained in the technical, legal and ethical parameters of appropriate camera and recorder use. Operators will receive a copy of this procedure and provide written acknowledgement that they have read and understood its contents by signing a confidentiality agreement.

f. Each authorized operator will have a distinctive login and password assigned to them.

5. Complaints

The College will respond to complaints regarding video surveillance as follows:

a. A complainant will submit the complaint, in writing, to the Manager, Records Management and Privacy (the Manager). This complaint will include the reason for making the complaint as well as the redress desired.

b. Within seven (7) days of receipt, the Manager will provide to the complainant acknowledgement that the complaint has been received.

c. The Manager will conduct an initial review of the complaint to determine if the complaint appears to have merit.

d. If the Manager determines that the complaint appears to have merit, the Manager will, within 30 days of receipt of the original complaint, convene a review group consisting of him or herself, the Vice-President, Administration and Finance, the Director, Facilities, and the Manager, Safety, Security and Emergency Management. This group will review the complaint and make a recommendation to the President as to whether the complaint is justified and, if so, a recommendation as to how the College should proceed.

e. The President will decide, within 45 days of receipt of the original complaint, the action to be taken, and communicate this decision to the review group.

f. The Manager will communicate this decision to the complainant within 60 days of receipt of the complaint.

g. If for any reason the Manager, the review group or the President are unable to meet the deadlines specified within these procedures, they are to communicate that fact and the reasons for the delay to the complainant without delay and in any case not later than the deadlines specified.

h. When the final decision has been made the Manager is to supervise any action taken by the College.

6. Privacy Breaches

British Columbia's Office of the Information and Privacy Commissioner outlines the following steps for responding to a privacy breach:

a. Contain the breach. Stop the leak of records, recover the information where possible, change the management practice if applicable, but generally do what needs to be done to stop the leakage of information. Designate a person to lead an investigation (normally the Manager, Records Management and Privacy).

b. Evaluate the risks. Determine the nature of the information leaked and the possible illegitimate uses for the leaked information. Determine what individuals were affected by the breach and what harm could potentially accrue to them. Determine the cause of the breach. For example, was the breach a result of a theft, or was it simply a loss? Is the breach a systemic problem or an isolated incident?

c. Notify those affected. Notification includes not only individuals whose personal information was leaked, but potentially the greater College community, law enforcement organizations, insurers, and regulatory bodies (including the Office of the Information and Privacy Commissioner).

d. Prevent. Investigate the cause of the breach and take whatever steps are necessary to prevent another breach.