ELECTRONIC SECURITY CLOSED CIRCUIT TELEVISION POLICY

EFFECTIVE DATE December 2003

RESPONSIBLITY FOR IMPLEMENTATION Director, Campus Operations

CROSS-REFERENCE Health and Safety Policy
Facility Policy
Records Management Policy
Freedom of Information and Protection of Privacy Act

POLICY STATEMENT

Grande Prairie Regional College utilizes electronic security closed circuit television surveillance measures to assist us to provide a secure environment for students and personnel and for the protection of assets.

GUIDELINES

1. The College has an obligation to notify the general public that activities on College grounds and in College facilities may be monitored, and will post signage to that effect.

2. The College may utilize overt surveillance systems in public or other areas both inside and outside of buildings to monitor activity for safety/security and for investigative purposes.

3. Covert surveillance systems may be authorized for specific incidents or investigations only. Such authorization must come from the Vice President of College Services or their designate.

For Management of Campus Operations in relation to the Electronic Security Closed Circuit Television Policy

DEFINITIONS:

Investigative Measures: may include the use of surveillances systems, individual interviews, authorized access to confidential and non-confidential files, reports, images and information, use of investigative products and devices, access to personal work/instructional/storage spaces and the use of police and external security services.

Surveillance System: refers to a mechanical or electronic system or device that enables continuous or periodic video recording, observing or monitoring of areas and spaces and individuals who may enter those areas or spaces.

Overt Surveillance Systems: refers to the open and unconcealed use of surveillance systems. Overt surveillance devices (cameras) are not masked, camouflaged or hidden from view.

Covert Surveillance Systems: refers to the secretive use of surveillance systems. Covert surveillance devices (cameras) may be masked, camouflaged or hidden from view.

Storage Device: refers to a videotape, DVD, computer disk or drive, CD ROM or computer chip used to store the recorded visual images captured by a surveillance system.

PROCEDURES:

1. All incidents or attempted incidents associated with criminal activity, security or personal safety must be reported immediately as indicated below:

    - Main Campus – reported to Campus Operations or during non-hours of operation or in the event that there is no one in Campus Operations, to Campus Security at 539-2700. For emergency situations, incidents can be reported directly to the local Police authorities (911) and then notify Campus Operations.

    - Off-Site Campuses – reported to the respective Chairperson, who will in turn notify Campus Operations as soon as possible. For emergency situations, incidents can be reported directly to the local police authorities (911) and then notify Campus Operations.

2. The Director, Campus Operations will inform the V.P. College Services of all reported incidents, other than those considered to be minor in nature. The V.P.

College Services will be informed of all investigations.

3. The Director, Campus Operations will respond to all reported complaints or incidents and will carry out internal investigations to gather information and/or rectify the situation. Where appropriate, the Director will utilize Campus Security Guards or contracted security personnel to assist in the investigation. Local Police authorities will be called in as required. The Director, Campus Operations will maintain a documented record of the investigation.

4. For investigative purposes, access to personal space and belongings and confidential information both paper and electronically stored, may be required. Access to information could include College, employee and student records, files and correspondence. Such access must be authorized at the Executive level.

5. When incidents or attempted incidents are of a major or criminal nature Campus Security will control the area, document the events and take pictures where necessary. The area may be secured and/or cordoned off with restricted access to protect any potential evidence until local Police authorities arrive.

6. In investigations, where covert surveillance systems are required they must be authorized by V.P. College Services or designate. Before being authorized, the use of surveillance must document rationale for meeting three tests and seven conditions as listed below:

   Covert Surveillance Tests:
   - There must be reasonable cause to use covert surveillance
   - There are no other reasonable investigative alternatives available
   - The level of intrusiveness does not out weigh any harm that could be done

   Covert Surveillance Conditions:
   - The respective Chair/Director /Executive has been consulted and the consultation has been documented and signed off
   - Mounting locations of devices and areas to be viewed are specifically identified and documented
   - Dates and times that equipment will be installed and removed are specified and documented
   - Dates and timings when activity will be monitored and/or recorded are specified and documented
   - Dates and timings that recorded activity will be viewed are specified and documented
   - Persons authorized to monitor activity and/or view recordings are identified and documented

- Names of all persons privy to the use of the covert surveillance are documented

In addition to the above, the Personal Impact Assessment (PIA) forms must be completed. (www.oipc.ab.ca/pia/template.)

7. When overt surveillance systems are installed in public spaces, workspaces or other areas inside a building, signage may be displayed at the entrances of the building so that persons entering the building are made aware that the building is under video surveillance.

8. Live and recorded images from a surveillance system shall be treated as confidential. Videotapes, computer disks, monitors, DVD's, CD ROM's or other such devices containing recorded images shall be stored in secured locations. Access to such locations shall be by authorized personnel only. The viewing of images from a surveillance system shall be restricted to only those persons authorized to do so by the Director, Campus Operations. Viewing shall be in areas with controlled access.

9. When local police are handling investigations Campus Operations will be their primary College contact point. Campus Operations will retain the names of the contacting Police Officers and the assigned police file number.

10. Unless required for a specific incident or investigation, the College will permanently erase or destroy all recorded visual images on its storage devices within 30 days from the date the images were recorded. Authorization to retain images longer must come from the V.P. College Services. Old storage devices must be securely disposed of by shredding, burning or magnetically erasing the information. Breaking open the storage device is not sufficient.

11. The College may for good and reasonable cause make and retain copies of video images and/or frames thereof that were recorded on storage devices for unspecified periods of time based on investigative circumstances. Authorization to make and retain copies must come from the V.P. College Services. The recorded information will be kept for at least one year after the decision is made.

12. When Police authorities request College recorded images for their investigative purposes, a storage device release form will be completed before any storage device is disclosed to such authorities. The form should state who took the device and when, under what authority, and if it will be returned or destroyed after use.

13. Electronic surveillance equipment such as video cameras shall be installed in identified public areas where surveillance is a necessary and viable detection or deterrence activity. Equipment should not monitor areas where the public and

employees have a reasonable expectation of privacy (e.g., change rooms and adult washrooms).

14. Electronic surveillance equipment shall not be positioned, internally or externally, to monitor areas outside a building, or to monitor other buildings, unless necessary to protect external assets or to address personal safety. Cameras shall not be directed to look through the windows of non-College buildings in the viewable vicinity or into College living areas.

Resource:
http://www3.gov.ab.ca/foip/other_resources/publications_videos/surveillance_guide.cfm