

OLDS COLLEGE POLICY

Olds College recognizes the need for Policies and Procedures, and the need for staff and students to be familiar with and follow such policies and procedures. It is the policy of the Board of Governors that breach of College Policies or Procedures shall result in disciplinary measures up to and including suspension or termination. This applies to all College staff and representatives.

CATEGORY:	A: General		
SUBJECT:	Electronic Surveillance Use		
POLICY NUMBER:	A32		
CROSS REFERENCE:			
NEW \ REVISED			
Board of Governors	Administrative Services Committee	Academic Council	Common Issues
Date: June 27, 2013	Date: June 18, 2013	Date:	Date:

POLICY STATEMENT

Olds College recognizes the need to balance an individual's right to privacy and the institution's duty to promote a safe environment and protect college assets.

A reasonable and limited degree of monitoring, as set forth in this Policy is appropriate and surveillance of public areas via closed circuit television (CCTV) or similar means of technology will be used at Olds College facilities.

This policy does not apply to legitimate uses of video cameras or recording devices for college promotion, instruction, research, or other non-surveillance purposes. This policy does not include the use of surveillance cameras or equipment used by police authorities.

DEFINITIONS

For purposes of this policy the following definitions make clear and distinct intentions for terminology included in the policy and procedures.

1. Electronic Surveillance – refers to a mechanical or electronic system or device that enables continuous or periodic video recording, observing or monitoring of personal information.
This does not include audio footage.
This does not include monitoring communications by means of computer, telephone, or radio.
2. FOIP – The Freedom of Information and Protection of Privacy Act (Alberta).
3. Staff – refers to all employees of the College, as well as those persons who perform a service to the College, an appointee or volunteer, or under a contract or agency relationship with the College.

4. Reception Equipment – refers to the equipment or device used to receive or record the personal information collected through a video surveillance system, including a camera or video monitor or any other video, physical or other mechanical, electronic, or digital device.
5. Storage Device – refers to a videotape, computer disk or drive, CD-ROM, computer chip, or other device used to store the recorded data or visual images captured by an electronic surveillance system.
6. Record – refers to personal information as defined in section 1(q) of the FOIP Act as a record of information in any form and includes notes, images, audio-visual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records. In the context of this policy and procedure, “record” includes digitally recorded or stored media such as images on video.
7. Disclosure – allow to be seen, the act of providing visual access of a record.
8. Release – relinquishment to another the possession of a record and/or to make available copies of records to someone other than staff designated within the policy.

SPECIFIC GUIDELINES

Implementation and use of surveillance systems at the College are to be in compliance with FOIP.

1. Location

Monitoring devices will only be located in public areas where those under surveillance have no reasonable expectation of privacy. All electronic surveillance shall be conducted in a professional, ethical, and legal manner.

2. Notification

Public areas with surveillance equipment will be signed accordingly to ensure that persons entering these areas are aware that cameras may be in operation.

3. Use of Surveillance Equipment

Receiving equipment will be secure. Only authorized persons will have access to receiving equipment. Authorized persons will access the recorded images only if there is a security based reason, if an incident has been observed, reported or is suspected to have occurred.

4. Use of Recorded Images

Disclosure

The recorded images may be disclosed to any of the following for the purposes of an incident that has been observed, reported or is suspected to have occurred:

- a. law enforcement agencies;
- b. staff or person(s) as designated by the Vice President Student and Support Services;

- c. relating to student conduct on or about Olds College property recordings may also be accessed by designates, as approved by the Vice President Student and Support Services, for Boards or administrators of Olds College partners;
- d. the individual who is the subject of surveillance in relation to an identified incident.

Release

Recorded images may be released to third parties or applicants in compliance with the provisions contained in FOIP and any rules or regulations there under.

5. Storage of Recorded Images

The College will provide reasonable security measures to prevent unauthorized access, disclosure, or release of the electronic surveillance records or live feed.

6. Disposal of Recorded Images

All recordings shall be disposed of in a secure manner unless they are archived as part of a permanent record.

IMPLEMENTATION AND ADMINISTRATIVE RESPONSIBILITY

The Vice President of Student and Support shall approve a Security Surveillance Plan annually.

This policy will be reviewed by the Vice President of Student and Support Services every 5 years.

OLDS COLLEGE PROCEDURES

Olds College recognizes the need for Policies and Procedures, and the need for staff and students to be familiar with and follow such policies and procedures. It is the policy of the Board of Governors that breach of College Policies or Procedures shall result in disciplinary measures up to and including suspension or termination. This applies to all College staff and representatives.

SUBJECT AND POLICY NUMBER	Electronic Surveillance Use A32	
NEW \ REVISED		
Common Issues	Administrative Services Committee	Academic Council

1. Scope

This procedure applies to all electronic surveillance located on Olds College proper and adjoining areas with the exception of devices used for instructional or research purposes. The purpose of this policy is to provide guidance in establishing the responsible use and development of a campus wide security system. Images collected may be used for police, legal, criminal, and/or civil proceedings.

2. Authority

- a. Olds College operating under the authority of the Post-secondary Learning Act (Alberta), collects personal information by Electronic Surveillance in accordance with the provisions of FOIP which permit:
 - i. Collection of personal information for the purpose of law enforcement;
 - ii. Collection of personal information that relates directly to and is necessary for an operating program or activity of the College.
- b. Violations regarding Electronic Surveillance monitoring and disclosure will result in disciplinary action, consistent with the rules and regulations governing employees of the College, up to and including dismissal or termination of contract.
- c. The Vice President of Student and Support shall approve a Security Surveillance Plan annually.
- d. The Vice President of Student and Support Services shall designate person(s) to manage and control the use and security of camera/surveillance system and data collected.

Primary Designate(s) shall:

- I. Maintain a current Security Surveillance Plan to include:
 - i. a list of fixed camera locations where electronic surveillance is employed;
 - ii. a list of temporary cameras locations where electronic surveillance is employed with record of the duration of installation;
 - iii. a catalogue of fixed camera location view to ensure the areas captured do not infringe privacy;

- iv. a general description of the technology and capabilities of each camera;
 - v. a list of individuals authorized to monitor and access the electronic surveillance;
 - vi. a list of individuals authorized to access electronic surveillance records;
 - vii. a Privacy Impact Assessment to assess the effects electronic surveillance may have on privacy and the ways in which any adverse effects can be mitigated.
- II. Authorize access to electronic surveillance or video monitors while they are in operation.
 - III. Authorize to extract footage from the recorded electronic surveillance for disclosure or release.
 - IV. Maintain a log for any retained footage (video/still) identifying the purpose for retention.

Secondary Designate(s) shall:

- I. Access to electronic surveillance or video monitors while they are in operation.
- II. Extract footage from the recorded electronic surveillance.
- III. Disclose records appropriately.
- IV. Maintain a log for any retained footage (video/still) identifying the purpose for retention.

3. Location

- a. Video cameras may be placed in selected public areas for the purpose of surveillance.
- b. The Vice President of Student and Support Services will review permanent camera locations to ensure the areas captured by the camera respect privacy.
- c. The Vice President Student and Support Services must approve locations of temporary cameras to be used for special circumstances. Temporary camera locations will be disclosed to the Dean and/or Supervisor of the area prior to the installation of the camera, unless otherwise approved by the President.
- d. Surveillance is to enhance security for students, faculty, staff, and visitors, in addition to providing protection of physical and livestock assets, and to improve effectiveness when dealing with nuisance, vandalism, or criminal acts by providing deterrence and detection. Legitimate activities involving Electronic Surveillance systems include, but are not limited to:
 - i. Protection of buildings and property - building perimeter, entrances and exits, lobbies and corridors, receiving docks, special storage areas, laboratories, cashier locations, locker banks, etc;
 - ii. Monitoring of access control systems - monitor and record restricted access transactions at entrances to buildings and other areas;
 - iii. Verification of security alarms - intrusion alarms, exit door controls, etc;
 - iv. Video patrol of public areas - parking lots, vehicle intersections or entrances, pedestrian walkways or hallways, etc;

- v. Criminal investigation - Robbery, burglary, and theft surveillance.

4. Public/Campus Notification

- a. Signs shall be posted to notify individuals that areas of campus may be under video surveillance.
- b. Where at all possible the language on signage will be consistent across the campus.

Signage will state:

- THIS BUILDING IS UNDER VIDEO SURVEILLANCE; or
- AREAS OF THIS CAMPUS ARE UNDER VIDEO SURVEILLANCE.

5. Installation/Purchase

- a. Olds College's Information Technology Department will be the initial contact point for purchase and/or installation.
 - i. All new installations in any location on campus must meet a standard as specified by Director Information Services to ensure that all cameras and devices integrate and are compatible with network/IT infrastructure and current software.
 - ii. All existing electronic surveillance or video recording systems will be evaluated for compatibility with the campus network and compliance with policy and procedures.
- b. Departments are responsible for the purchase, maintenance, upgrade of equipment installed in their facilities, and any incremental cost associated to install.
 - i. Costs to a Department purchase shall include, but not limited to: support of the security network infrastructure supporting the campus's operations, archival video or data retrieval.
 - ii. IT and Campus Facilities gives prior agreement to the installation. The actual installation may be by an external contractor.
 - iii. All systems or components are to be purchased from an Olds College approved vendor/contractor.

6. Use/Management of Recorded Images

- a. Authorized persons only will access the recorded images only if there is a security based reason, if an incident has been observed, reported or is suspected to have occurred.
- b. Electronic surveillance shall not be used as an instrument for monitoring day to day employee performance or for supervision. This does not preclude the use of video recordings/captured images of the workplace for criminal investigation purposes or as evidence for prosecution of criminal acts discovered in the workplace.
- c. Legitimate use of records include, but are not limited to, the following:
 - i. security or law enforcement purpose;

- ii. a legal proceeding;
 - iii. the provision of evidence in support of any inquiry or action associated with criminal and/or anti-social activity on campus property or the misuse of campus space or equipment.
- d. Where a person has been the subject of electronic surveillance, the person has the right to view her or his recorded images, unless refusal to allow access is required by FOIP or included in any of the discretionary exclusions to the general right of access, as set forth in FOIP. Any such requests for disclosure or release shall be processed by the Olds College FOIP Coordinator, in collaboration with primary designate(s) as approved by the Vice President Student and Support Services.

7. Access, Protection, and Retention

- a. All video surveillance is considered a record of Olds College, and therefore under the custody and control of Olds College.
 - i. Olds College's Information Technology Department is responsible for the secure storage of recorded images on the network system.
 - ii. Corresponding Department heads (Supervisor, Manager, Dean, Director) are responsible for the secure storage of extracted images protected as a confidential record.
- b. The College will provide reasonable security measures to prevent unauthorized access to the video surveillance.
 - i. Only authorized access to electronic surveillance or reception equipment.
- c. No attempt shall be made to alter any part of a video recording.
- d. Videos are initially recorded in reception equipment on a data collection media. Information on such a media is retained until such time that it becomes full and then the oldest video segments are overwritten by the newest segments. Recorded video images will be erased, deleted, or otherwise permanently eliminated within 30 days or as soon as segments are overwritten on the device, unless the video footage is being retained as part of a police investigation, court proceeding (criminal or civil), or internal investigation.
- e. In circumstances where recording from the surveillance cameras will be used to make a decision affecting an individual whose personal information has been captured on the surveillance images, the recorded personal information shall be maintained for at least one (1) year from the date that the decision affecting the individual has been made.
 - i. Recordings relevant to the investigation of an incident will be saved onto another permanent media, and may be retained by the college indefinitely as a permanent archive.

8. Protection of Information and Disclosure

- a. Personal information contained on the storage devices/recordings shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual whose personal information has been captured, or as required by law.
- b. All records that have been saved pending the final outcome of an incident investigation shall be numbered, dated, and retained in a secure location.
- c. Recorded images may also be used by the Boards or administrators of the CLC partners/tenants, Olds High School, or Housing contractor, as evidence in disciplinary action relating to student conduct on or about Olds College property.
 - i. Olds High School Principal authorizes appropriate disclosure and use of identified CLC related devices;
 - ii. Recorded images of non-CLC devices by partners identified in 8(c) not relating to student conduct shall be considered under a FOIP request.
- d. Information obtained through monitoring and/or recording will only be released in accordance with this policy, FOIP, or as required by law.

9. Disposal or Destruction of Recordings

- a. All recorded images shall be disposed of in a secure manner unless they are archived as part of a permanent record.
- b. All video recordings shall be disposed of in a safe and secure manner as directed by Olds College Information Technology Department.