ELECTRONIC SURVEILLANCE USE

This procedure is governed by its parent policy. Questions regarding this procedure are to be directed to the identified Procedure Owner.

Category:	B. Administration
Parent Policy:	B02
Approval Date:	November 30, 2023
Effective Date:	November 30, 2023
Procedure Owner:	Director, Residence & Ancillary Services Director, Information Technology

Overview:

This procedure applies to all electronic surveillance located on Olds College of Agriculture & Technology (the "College") property and adjoining areas with the exception of devices used for instructional or research purposes. The purpose of this procedure 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.

Procedures:

Authority

1. The College, operating under the authority of the Post-Secondary Learning Act (Alberta), collects personal information by electronic surveillance in accordance with the provisions of the Freedom of Information and Protection of Privacy Act (FOIP) which permit:
    a. Collection of personal information for the purpose of law enforcement.
    b. Collection of personal information that relates directly to and is necessary for an operating program or activity of the College.
2. Violations regarding electronic surveillance monitoring and disclosure, and/or any tampering with or vandalism to cameras or recording equipment will result in disciplinary action, consistent with the rules and regulations governing employees or students of the College, up to and including dismissal or termination of contract.
3. The Procedure Owner(s) shall submit an annual Security Surveillance Plan that includes camera locations and access permissions to the Vice President, Student Experience.
4. The Procedure Owner(s) shall designate staff to manage and control the use and security of the camera/surveillance system and data collected.
    a. Procedure Owners(s) shall:
        i. Authorize access to electronic surveillance or video monitors while they are in operation.
        ii. Authorize access to extract footage from the recorded electronic surveillance for disclosure or release.

5. Designated Staff shall:
    a. Prepare an annual Security Surveillance Plan to include:
        i. A list of fixed camera locations where electronic surveillance is employed.
        ii. A review of fixed camera locations to ensure the areas captured to not infringe on the reasonable expectation of privacy.
        iii. A list of individuals authorized to monitor and access the electronic surveillance and/or recorded footage.
        iv. 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.
    b. Grant live view access to electronic surveillance or video monitors while they are in operation.
    c. Grant access to view or extract recorded footage.
    d. Extract footage from the recorded electronic surveillance on request.
    e. Any persons that extract recorded footage shall maintain a log for any retained footage (video/still) identifying the purpose for retention.
    f. Disclose records appropriately.

Location

1. Video cameras may be placed in selected public areas for the purpose of surveillance.
2. Camera locations will ensure the areas captured by the camera respect reasonable expectations of privacy.
3. The Vice President, Student Experience 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.
4. Surveillance is to enhance security for students, faculty, staff, and visitors. In addition, to provide 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:
    a. Protection of buildings and property - building perimeter, entrances and exits, lobbies and corridors, receiving docks, special storage areas, laboratories, cashier locations, locker banks, etc.
    b. Monitoring of access control systems - monitor and record restricted access transactions at entrances to buildings and other areas.
    c. Verification of security alarms - intrusion alarms, exit door controls, etc.
    d. Video patrol of public areas - parking lots, vehicle intersections or entrances, pedestrian walkways or hallways, etc.
    e. Criminal investigation - robbery, burglary, and theft.

Public/Campus Notification

1. Signs shall be posted to notify individuals that areas of campus may be under video surveillance.
2. Where at all possible, the language on signage will be consistent across the campus.
    a. Signage will state:
        i. This building is under video surveillance; or

ii. Areas of this campus are under video surveillance.

Installation/Purchase

1. The College's Information Technology Department will be the contact point for purchase and/or installation.
    a. All new installations in any location on campus must meet a standard as specified by the Director, Information Technology to ensure that all cameras and devices integrate and are compatible with network/IT infrastructure and current software.
    b. All existing electronic surveillance or video recording systems will be evaluated for compliance with policy and procedures.
    c. IT and Campus Facilities give prior agreement to the installation. The actual installation may be by an external contractor.

Use/Management of Recorded Images

1. Authorized persons only will access the recorded images if there is a security-based reason; if an incident has been observed, reported or is suspected to have occurred.
2. 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.
3. Legitimate use of records include, but are not limited to the following:
    a. Security or law enforcement purpose.
    b. A legal proceeding.
    c. 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.
4. Where a person has been the subject of electronic surveillance, the person has the right to view their 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 College FOIP Coordinator, in collaboration with primary designate(s) as approved by the Vice President, Student Experience.

Access, Protection, and Retention

1. All video surveillance is considered a record of the College, and therefore under the custody and control of the College.
    a. The College's Information Technology Department is responsible for the secure storage of recorded images on the network system.
    b. Corresponding Department Heads (Supervisor, Manager, Dean, Director) are responsible for the secure storage of extracted images protected as a confidential record.
2. The College will provide reasonable security measures to prevent unauthorized access to the video surveillance.
    a. Only authorized access to electronic surveillance or reception equipment.
3. No attempt shall be made to alter any part of a video recording.
4. 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. 5. 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 year from the date that the decision affecting the individual has been made. a. 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. **Protection of Information and Disclosure** 1. 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. 2. All records that have been saved pending the final outcome of an incident investigation shall be numbered, dated, and retained in a secure location. 3. Recorded images may also be used by the Boards or Administrators of the Community Learning Campus (CLC) partners/tenants, Olds High School, as evidence in disciplinary action relating to student conduct on or about College property. a. Olds High School Principal authorizes appropriate disclosure and use of identified CLC related devices. 4. Information obtained through monitoring and/or recording will only be released in accordance with this policy, FOIP, or as required by law. **Disposal or Destruction of Recordings** 1. All recorded images shall be disposed of in a secure manner unless they are archived as part of a permanent record. 2. All video recordings shall be disposed of in a safe and secure manner as directed by the College's Information Technology Department.
Definitions:	
Related Information:	
Review Period:	3 years
Revision History:	New: June 2013 Revised: November 2023