Title of the Policy: Surveillance Policy

**Functional Area:** University Police

**Applies To:** All Faculty and Staff

**Policy Reference(s):**

**Number:** Version 1.0

**Date First Issued:** March 15, 2016

**Date Last Reviewed:** This is the first Policy review for this topic.

**Page(s):** 6

---

**Responsible Person**

Responsibility for oversight of security cameras and associated policies, standards, and procedures, is assigned to the Chief of Police and the Vice President for Business and Finance.

---

**Purpose / Rationale**

Armstrong State University is committed to enhancing the quality of life of the campus community by integrating the best practices of safety and security with technology. A critical component of a comprehensive security plan is the utilization of a security camera system. The surveillance of public areas is intended to aid in criminal investigations and assist in protecting the safety and property of the Armstrong community. This policy addresses the university’s safety and security needs while respecting and preserving individual privacy.

The purpose of this policy is to regulate the use of security cameras used to observe and record public areas for the purposes of safety and security. The existence of this policy does not imply or guarantee that cameras will be monitored in real time – 24 hours a day, 7 days a week.

---

**Definitions**

As used within this policy, the following terms are defined as follows:

**Security camera:** A camera used for monitoring or recording public areas for the purposes of enhancing public safety, monitoring restricted areas or equipment, to discourage theft and other criminal activities, and for preventing, investigating, and resolving incidents. The most common security cameras rely on closed circuit television. This does not include body cameras assigned to police officers.

**Security camera monitoring:** The real-time review or watching of security camera feeds.
Security camera recording: A digital or analog recording of the feed from a security camera.

Security camera systems: Any electronic service, software, or hardware directly supporting or deploying a security camera.

All references to the Chief of Police refer to the head of the Armstrong Police Department or his or her designate.

Policy

The Armstrong University Police Department (UPD) has the authority to select, coordinate, operate, manage, and monitor all campus security surveillance systems pursuant to this policy. All campus surveillance cameras, except those listed below will be managed by UPD according to this policy. UPD’s responsibilities include:

1. Creation, maintenance, and review of a campus strategy for the procurement, deployment, and use of security cameras, including this and related policies;
2. Designation of the standard campus security camera system or service;
3. Authorizing the placement of all security cameras;
4. Authorizing the purchase of any new security camera systems;
5. Reviewing existing security camera systems and installations and describing required changes to bring them into compliance with this policy;
6. Creating and approving campus standards for security cameras and their use;
7. Creating and approving the procedures for the use of security cameras.

All existing uses of security camera systems will be required to comply with the policy by July 1, 2016.

It is the policy of the University that:

Security cameras will be used in a professional and ethical manner in accordance with university policy and local, state and federal laws and regulations. Security cameras may be installed in situations and places where the security and safety of either property or persons would be enhanced. Cameras will be limited to uses that do not violate the reasonable expectation of privacy as defined by law. Where appropriate, the cameras may be placed campus-wide, inside and outside buildings. Although the physical cameras may be identical, the functions of these cameras fall into three main categories.

A. Property Protection: Where the main intent of the camera is to capture video and store it on a remote device so that if property is reported stolen or damaged, the video may show the perpetrator. Examples: an unstaffed computer lab, an unstaffed science lab, or a parking lot.

B. Personal Safety: Where the main intent of the camera is to capture video and store it on a remote device so that if a person is assaulted, the video may show the perpetrator. Examples: a public walkway or a parking lot.

C. Criminal Investigations:
• Any use of video recording equipment must conform to state and federal laws and be managed in a professional, ethical manner.
• No video surveillance or recording equipment may be installed on campus without the approval of the Vice President for Business and Finance and in cooperation with the Chief of UPD unless explicitly excluded from this policy (see exceptions below).
• Information obtained through video surveillance recordings will be used only for security and law enforcement. Only those responsible for investigation and enforcement of laws/policies will have access to the recorded video.
• Virtual or fake cameras cannot be installed on campus

Images recorded by security camera systems are considered sensitive information whose confidentiality, integrity, and availability should be protected. Security camera recording will be considered university data that falls under the stewardship of the Vice President for Business and Finance. Security camera systems will be required to implement security safeguards appropriate to the sensitivity, criticality, and level of identified risks of stored video images and recordings. Covert cameras are hidden or concealed with no signage and usually are installed for a specific and targeted intent. Only UPD may install covert cameras for criminal investigations. Such surveillance must be authorized in writing by the Vice President for Business and Finance prior to the start of the surveillance.

**Related Procedures**

Procedures:

1. Access and Use
   a. Only authorized personnel, as determined by this policy or authorized by the Vice President for Business and Finance or designee, will be involved in, or have access to surveillance camera data.
   b. The use of dummy or placebo cameras is prohibited.
   c. University Police will have access to all surveillance camera data from the Armstrong Police Department office location.
   d. When an incident is suspected to have occurred, only authorized personnel may review the images from surveillance camera data.
   e. All requests for the release of surveillance records must be authorized by the University Counsel and the Vice President for Business and Finance.
   f. In general, the University will not permit either the installation or use of cameras as a tool to monitor routine performance or management issues involving university personnel or the use of personal “webcam” or similar technology for surveillance purposes. Employees of any department with surveillance cameras shall be notified of such installation unless the cameras are part of a criminal investigation.
   g. Video monitoring will be conducted only in areas where the public does not have a reasonable expectation of privacy.
h. In consultation with University Counsel, video surveillance implementations and policy exceptions will be reviewed by the Vice President for Business and Finance and the Chief of UPD on an annual basis.

2. Retention of Security Camera Recordings

   a. Security camera recordings will be retained for a period of no less than thirty (30) and no longer than sixty (60) days. This retention period may be extended at the request of University Counsel or the Chief of Police or as required by law.

   b. Security camera recordings can be stored on either local enterprise-class storage located in the Armstrong data center or on designated Cloud service providers. Such service providers include, but are not limited to: The University System of Georgia, Amazon Web Services, or a security camera system vendor who is contracted with Armstrong State University to provide such services.

   c. In general, the Chief of Police is responsible for the operation and use of the system. Typical areas of responsibility include all functional uses of the system, video archive settings, aiming of cameras equipped with such functionality, creation of user accounts, setting of user account permissions, training of personnel, and the primary point of contact for vendor communications.

Security Camera Placement

1. Armstrong Police will assess new camera locations based upon proposals and recommendations for new camera installations and specific incidents supporting camera installation. Armstrong Police may then establish temporary or permanent security cameras in public areas of the campus subject to the approval of the Vice President of Business and Finance.

2. Legitimate safety and security purposes include, but are not limited to, the following:

   a. Building perimeters, entrances and exits, lobbies and corridors, elevators, receiving docks, special storage areas, laboratories, cashier locations, etc.

   b. Monitoring and recording of access control systems

   c. Monitoring and recording restricted access transactions at entrances to buildings and other areas

   d. Verification of security alarms

   e. Intrusion alarms, exit door controls, hold-up alarms, etc.

   f. Electronic patrol of public areas

   g. Transit stops, parking lots, public (enclosed and unenclosed) streets, shopping areas, vehicle intersections, etc.

   h. Criminal investigations

   i. Monitoring of pedestrian and vehicle traffic and vehicles in traffic areas at intersections.

3. Security cameras may not be used in private areas of the campus pursuant to legal restrictions.

   1. Private areas include offices, classrooms not used as labs, medical and mental therapy or treatment rooms, occupied residence hall rooms, bathrooms, shower areas, locker and changing rooms, and other areas where there is a reasonable expectation of privacy.
Where security cameras are permitted in private areas, they will, to the maximum extent possible, be narrowly used to protect money, real or personal property, documents, supplies, equipment, or pharmaceuticals from theft, destruction, or tampering.

4. To the maximum extent possible security cameras shall not be used to get close-up video through the windows of any private residential or office space unless specifically authorized by the Vice President of Business and Finance and University Counsel.

5. Security cameras will not be used for any unofficial purpose.

6. The conduct of surveillance monitoring or recording, and use of surveillance cameras must follow Georgia and federal law.

Review of Security Camera Recordings

University Police employees, ITS employees, or subcontractors under the direction of the Armstrong Police Department are responsible for the daily operation of the cameras. They will follow all university policies, procedures, and guidelines in the monitoring of CCTV cameras. No staff other than staff trained in the use of the CCTV system will operate cameras at any time. The Policy Chief may appoint a person to audit the monitoring operations, including image storage.

Monitoring of Security Camera Feeds

University security cameras are not monitored continuously under normal operating conditions but may be monitored for legitimate safety and security purposes that include, but are not limited to, the following: high risk areas, restricted access areas/locations, in response to an alarm, special events, and specific investigations authorized by the Chief of Police or designee. Access to live video or recorded video from cameras shall be limited to, the Armstrong Police Department and other persons authorized by the Chief of Police or designee. The copying, duplicating and/or retransmission of live or recorded video shall be limited to persons authorized by the Chief of Police or designee.

Notification Requirements

Buildings with security cameras may have signs at the primary building entrances displayed that provide reasonable notification of the presence of security cameras. All proposals for the deployment of security cameras will include proposed sites for the placement of notifying signs. The design, size, placement of the signs and the text on the signs will be subject to the review and approval of the Director of Facility Services.

Use of Recordings

Personnel are prohibited from using or disseminating information acquired from university security cameras, except for official purposes. All information and/or observations made in the use of security cameras are considered confidential and can only be used for official university and law enforcement purposes. This use extends to their release by the Armstrong Police Department to external law enforcement agencies. Records of the access to and release of security camera recordings must be sufficient so as to validate compliance with this policy.
Security camera recordings may not be used in the course of personnel investigations such as those related to (but not limited to) work place attendance or work quality, except as authorized by the Vice President for Business and Finance.

Public Records requests for video recordings are directed to the University Counsel.

**Exceptions**

This policy does not apply to the use of video for non-surveillance purposes, examples include:

1. The academic use of cameras for educational purposes
2. Cameras used for research purposes, which are subject to appropriate Institutional Review Board policies regarding human subjects
3. Cameras used for journalistic purposes
4. Cameras used for capturing public events and performances including athletic events or practices
5. Construction web cameras
6. Webcams used for purposes of communication between specific persons
7. Automated teller machines (ATMs) installed by third party vendors, which may utilize cameras
8. Video conference equipment installed on campus