

Somerset Community College

Video Surveillance Policy

The purpose of this Policy is to outline guidelines for the responsible use of security cameras owned and operated by Somerset Community College campuses. This Policy seeks to balance the safety and security of the College community with the privacy interests of all employees, students, guests and visitors. This Policy is not intended to address the use of video equipment for academic, media, or operational purposes. Additionally, this Policy shall not apply to monitoring equipment installed in ATMs by sponsoring banks or continuing vendors, such as Barnes and Noble.

Policy

Somerset Community College deploys security cameras on its campus solely to advance legitimate public safety and security interests, including, without limitation:

- Protection of individuals, property and buildings
- Investigation of criminal activity
- Monitoring of building access
- Confirmation of security and safety alarms
- Situational awareness of campus events

The use of security cameras shall be conducted at all times in a professional, ethical, and legal manner. Individuals operating or using footage from security cameras shall do so in accordance with this policy and all relevant College and KCTCS policies, including, but not limited to, those governing sexual harassment and discrimination. Operators of security cameras must also comply with any applicable federal, state, and local laws. This Policy places limits on the use of surveillance equipment and recordings generated by such equipment to protect the reasonable privacy interests of the College community and visitors to the College's campuses.

Scope

This policy applies to all personnel and every department of Somerset Community College in the use of security cameras and their video monitoring and recording systems. College employees may not operate or use recordings generated by security cameras unless authorized through their job descriptions or in writing by the college president. Unauthorized operation or use of recordings may result in disciplinary action up to and including termination. This policy does not apply to students except in cases where students are also employees who are authorized to use security cameras as indicated in this paragraph.

This policy shall apply to the installation of security cameras in situations and places where the security and safety of either property or persons would be enhanced. This policy shall not permit cameras to be placed or used in places or manners that 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 two main categories:

A. Property Protection: Where the main intent 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: a computer lab, an unstaffed science lab, or a parking lot.

B. Personal Safety: Where the main intent 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.

General Principles

Information obtained from the cameras shall be used primarily for campus policy enforcement, including, where appropriate, student judicial actions. When legally appropriate, security cameras and the recordings generated may be used to assist local law enforcement and campus/local safety and security personnel. Information gathered through the use of security cameras must be handled with an appropriate level of security to protect against unauthorized access, alteration, or disclosure.

All appropriate measures must be taken to protect an individual's right to privacy and hold college information securely through its creation, storage, transmission, use, and deletion.

All camera installations and the recordings made by those installations are subject to federal and state laws.

Placement of Cameras

The locations where cameras are installed may be restricted access sites such as a departmental computer lab; however, these locations are not places where a person has a reasonable expectation of privacy. Cameras will be located so that personal privacy is maximized. The college will provide signs or other reasonable notification to ensure individuals are aware of video monitoring in areas where security cameras have been installed or are in use.

Camera positions, which include views of restrooms, shall be limited. The view must not violate decency standards or any reasonable expectation of privacy.

When the College President and his/her security personnel find that reasonable suspicion exists that activity violating policy or law has occurred in an area with a heightened expectation of privacy, the College President, in consultation with the KCTCS Office of General Counsel, may authorize, in writing, the use of security cameras in such areas. Absent the steps in this paragraph, security cameras shall not be used in areas of heightened expectations of privacy.

Cameras shall at no time be permanently fixed in areas with the highest expectation of privacy. Authorized employees may only temporarily use security cameras in such areas when the Office of General Counsel has approved such use in writing. The use of cameras in such areas will only be based upon a likelihood that serious administrative or criminal action shall result from the recording generated. At times, it may be necessary for law enforcement to approve the use of cameras in these areas, and in those cases, the Office of General Counsel shall take the lead in coordinating

these efforts. Areas with a heightened expectation of privacy include, but may not be limited to, the following:

- Faculty or Staff private offices
- Bathrooms
- Locker rooms
- Other locations in which the reasonable expectation of privacy outweighs the interest in recording, as determined by the College President.

As stated above, some form of notification to the public of possible video surveillance shall be required, and all video camera installations should be visible to the public. Exceptions to notification and visibility are those where an investigation of serious violations of policy or law are underway and have been approved as required above.

The exact location, number and function of all cameras will generally be considered confidential for security purposes and not be released to the public, guest or employee unless required by law.

Access and Monitoring

All recording or monitoring of individual or group activities through the use of college security cameras will be done in a manner consistent with KCTCS policies, college policies and state and federal laws. Monitoring or recording will not be based on the subjects' personal characteristics, including age, color, disability, gender, gender identity or presentation, national origin, race, religion, sexual orientation, or other protected characteristics. Furthermore, all recording or monitoring will be conducted in a professional, ethical, and legal manner.

College security cameras are not generally 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, maintenance purposes, functionality purposes and specific investigations authorized by the Chief of Operations.

When an incident is reported, the personnel responsible for the area in question may request Security to review the images from the camera. As circumstances require, the Chief of Operations may authorize others to review images. In cases where the recording will be used for personnel or student conduct actions, the Office of General Counsel shall approve such use. To ensure that recordings are legally able to be authenticated and remain viable for administrative or legal action, a record log will be kept of all instances of access to, and use of, recorded material.

Requests for access to view video are made to the Chief of Operations. The request should include which camera output and the purpose for the access consistent with this policy. Any request pursuant to law enforcement investigations, subpoena, or the Kentucky Open Records Act shall be approved through the Office of General Counsel.

Appropriate Use and Confidentiality

Personnel are prohibited from accessing, viewing, using, or disseminating information acquired from college 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 college and law enforcement purposes upon the approval of the Chief of Operations, KCTCS Office of General Counsel, or the College President. Violation or abuse of this policy may result in disciplinary action, up to and including termination of employment. It may also subject the violator to criminal and civil liability for which neither the college nor KCTCS shall protect or represent the violator. Personnel are required to know and follow this policy.

Use of Cameras for Investigations that may Result in Administrative or Criminal Action

Mobile or hidden video equipment may be used only when authorized as described earlier in this policy. The use of mobile or hidden equipment shall comply with this and all relevant college/KCTCS policies as well as with all statutory and case law, both state and federal. Generally, such use shall be limited to instances of significant risk to public safety, security and property and shall be authorized by the Office of General Counsel.

Training

Camera control operators shall receive a copy of this policy and provide written acknowledgment that they have read and understood its contents.

Operation

Video surveillance will be conducted in a manner consistent with all existing college policies. Cameras will record but will not be monitored 24-7. Camera control operators shall monitor based on suspicious behavior, not individual characteristics. Camera control operators shall not view private rooms or areas through windows. Abuse of standard operating policies or inappropriate camera control operations may result in disciplinary action, up to and including termination of employment.

Storage and Retention of Recordings

All recorded video images remain the property of Somerset Community College. Recordings shall be securely maintained for approximately 30 days unless the recording device has limited storage space. In all cases, the recordings must be maintained at least 7 days and if used in personnel actions, student judicial proceedings, or other administrative or criminal proceedings, shall be kept until all appeals on actions are complete. As stated above, recorded images may be used as evidence in on-campus student judicial proceedings, employment actions, or for any other lawful purpose. Recorded images are subject to Kentucky open records law. Recordings may be released, in accordance with the Federal Educational Rights and Privacy Act (FERPA), to local law enforcement authorities in furtherance of an investigation into a criminal incident or motor vehicle accident. Individual students and employees are not permitted to review stored video images except in accordance with open records law or as a result of proper discovery in a legal proceeding.

Priority of Policy: Somerset Community College is part of the Kentucky Community and Technical College System (KCTCS), which is governed by the KCTCS Board of Regents. Accordingly, any provision of college policy or procedure inconsistent with the regulations, policies, or procedures of the KCTCS Board of Regents or KCTCS are void and shall have no force or effect, and those of the Board of Regents or KCTCS shall control.

In order to meet the continuously evolving interests of our students, the college, and the community, the college may modify this policy at any time, with or without advanced notice.