

COLLEGE SECURITY CAMERA POLICY

College Security Camera Policy

Effective July 22, 2020

<u>Purpose</u>

St. Francis College is committed to enhancing the quality of life of the campus community by integrating the best practices of safety and security with technology. As a result of that commitment, we have installed security cameras to various locations throughout our campus. St. Francis College respects the privacy of the college community members and is sensitive to balancing that privacy with safety needs on its campus. The deployment of cameras is supported and approved by The Student & Faculty Advisory Committee / Assistant Director of Campus Safety Security. The Assistant Director & The Advisory Committee are responsible for the oversight and approval of camera locations.

Security cameras are actively monitored and are used exclusively for campus safety and security purposes. St. Francis College employs a security camera system in order to deter crime; identify potential criminal activity; investigate criminal activity and violations of policies, procedures and rules applicable to St. Francis College; and to enhance safety for the campus community. This policy addresses St. Francis College's safety and security needs while respecting and preserving individual privacy.

To ensure the protection of individual privacy rights in accordance with St. Francis College's values as well as state and federal laws, this policy is adopted to formalize procedures for the installation of video surveillance equipment and the handling, viewing, retention, dissemination, and destruction of video surveillance records. The purpose of this policy is to regulate the use of security camera systems used to observe and record public and restricted areas for the purposes of safety and security.

Policy

All security camera footage is considered college records. Security camera footage will be securely stored in order to prevent tampering and will be managed by the Department of Campus Safety & Security. Technical support for camera system and stored security camera footage will be provided by the Technology Services department. The Department of Campus safety and security must authorize the use duplication, or release of security camera footage. Any requests to view camera footage must be submitted to the Department of Campus Safety & Security.

The Department of Campus Safety & Security shall monitor developments in the law and in security industry practices to ensure that security camera surveillance is consistent with best practices and complies with all federal and state laws.

St. Francis College Student & Faculty Advisory Committee and the Assistant Director of Campus Safety & Security will review proposals and recommendations for camera installations and will also review specific camera locations to determine that the perimeter of view of fixed location cameras conforms to this policy.

The Dean of Students Office will review any complaints regarding the utilization of surveillance camera systems and determine whether there are any violations of this policy.

The Dean of Students will review all third-party requests to release records obtained through security camera surveillance. The College may seek consultation and advice from its Legal Counsel as needed related to these requests prior to the release of any security camera surveillance records to third-parties. Security camera surveillance records will generally not be released to the public, students, employees, or parents. Security camera surveillance records College are record which may be subject to administrative regulations concerning the confidentially of student identities. While the Assistant Director of Campus Safety & Security will typically review the security camera footage, the College reserves its right to allow individuals to view security camera footage if that is a necessary action as part of an investigation of a crime, code of conduct violation, significant campus safety, concern, or campus policy violation.

General Principles

Security Cameras are actively monitored Security Officers. Personnel approved to monitor security camera videos should receive training in effective, legal and ethical use of the monitoring equipment. Security camera footage will be reviewed only upon report of a crime or violation.

Information obtained from security cameras shall be used exclusively for campus policy enforcement, including, student judicial functions or to assist local law enforcement

investigations campus/local crime. Security camera footage must be handled with an appropriate level of safety 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 and records securely through their creation, storage, transmission, use, and deletion. All security camera installations and subsequent camera use is subject to federal and state laws.

Placement of Cameras

St. Francis College reserves the right to place cameras on campus where necessary and appropriate. Security cameras will be located so that personal privacy is protected. No audio shall be recorded. Camera positions and views of residential housing shall be limited to external areas. The view of a residential housing facility must not violate the standard of a reasonable expectation of privacy as defined by state and federal law. Except as necessary for criminal investigation and except as in accordance with the terms of warrant, security cameras will not be installed in private areas which include, but are not limited to: residence hall rooms, bathrooms, shower area, locker and changing rooms and private offices.

All video camera installations should be visible. The exact location, number and function of all cameras will generally be considered confidential for security purposes and not be released to the general public, guests or employees. The College reserves the right to place cameras in areas that are not open to the campus or general public (e.g., closed buildings or secured areas).

Anyone who tampers with video equipment will be subject to disciplinary action through the Dean of Students Office.

Access and Monitoring

All recording or monitoring of activities of individuals or groups by College security cameras will be conducted in a manner consistent with College policies and; state and federal laws. Monitoring will not be based on the subjects' personal characteristics, including age, color, disability, gender, 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. All personnel with access to College security cameras should be trained in the effective, legal, and ethical use of monitoring equipment.

When an incident is reported, the personnel responsible for the area in question may request the Department of Campus Safety & Security to review the surveillance footage from the security camera. As circumstances require, the Dean of Students may authorize others to review surveillance footage. A log will be kept of all instances of

access to, and use of, recorded material. This log will be discarded at the end of each academic year.

Appropriate Use and Confidentiality

Personnel are prohibited from using or disseminating information acquired from College security cameras, except for official purposes. All information gathered and/or observations made through the use of security cameras is considered confidential and can only be used for official College and law enforcement purposes upon the approval of the Dean of Students / Director of Campus Safety & Security or their designee. Personnel are expected to know and follow this policy.

Use of Cameras for Criminal Investigations

The use of video equipment may be used in criminal investigations on behalf of the College. Individuals or agencies from outside of the College must request access to view materials in accordance with our policies governing student records. Video records may be destroyed within seven (30) days at the conclusion of any investigation and subsequent hearing process.

Exceptions

This policy does not apply to cameras used for academic purposes. Cameras that are used for research, communications, or class projects would be governed by other policies involving human subjects and are, therefore, excluded from this policy.

Safety and Security Camera Acceptable Use Policy

This policy does not address the use of student/employee personal cameras, webcams, videotaping events, or live streaming for general use by the College. This policy also does not apply to the use of video equipment for the recording of public performances or events, interviews, or other use for broadcast or educational purposes. Examples of such excluded activities would include videotaping of athletic events for post-game review, videotaping of concerts, plays, and lectures, live stream activity, or videotaped interviews of persons. Automated teller machines (ATMs), which may utilize cameras, are also exempt from this policy.

Procedures

Departments requesting security cameras will be required to follow the procedures outlined in this policy.

Training

Security camera control operators shall be trained in the technical, legal, and ethical parameters of appropriate camera use. Security 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 federal and state law as well as all existing College policies. Security camera control operators shall monitor based on suspicious behavior, not individual characteristics. Security camera control operators shall not view private rooms or areas through windows. All operators and supervisors involved in video surveillance will perform their duties in accordance with this policy. Abuse of standard operating policies or inappropriate camera control operations will result in disciplinary action.

Storage and Retention of Recordings

No attempt shall be made to alter any part of any surveillance recording. Surveillance centers and monitors will be configured to prevent camera operators from tampering with or duplicating recorded information without authorization.

All surveillance records shall be stored in a secure location for a period of 30 days and will then promptly be erased or written over unless retained as part of a criminal investigation or court proceedings (criminal or civil), or other bona fide use as approved by the Dean of Students. Individual departments shall not store video surveillance recordings.

A log shall be maintained of all instances of access to or use of surveillance records. The log shall include the date and identification of the person or persons to whom access was granted.