SUNY Cobleskill Electronic Surveillance Policy

PREAMBLE:
The purpose of this policy is to regulate the use of electronic surveillance and recording of public and restricted areas for the purposes of safety and security.

SUNY Cobleskill reserves the right to place cameras on campus where necessary and appropriate. This policy applies to all personnel, departments, offices, and other subdivisions of the College in the use of electronic recording and surveillance.

University Police has the primary responsibility for crime prevention, law enforcement, and other public safety and security matters on the campus and other college-owned property. Hence, University Police will control the cameras and recordings and have the primary responsibility for enforcing the policy. University Police is committed to enhancing its public safety efforts through the use of electronic surveillance under appropriate circumstances.

SUNY Cobleskill respects the privacy of university community members and is sensitive to balancing that privacy with safety needs on campus. Cameras extend the protection of University Police, even when officers are not in an immediate area.

Cameras are not a guarantee of safety, but are a tool that assists University Police.

Cameras protect campus community members from dangers by serving as deterrents and expediting investigations.

This policy does not apply to legitimate academic use of cameras for educational purposes, to cameras used for journalism, to private cameras owned and operated by members of the campus community, or to security cameras installed by authorized financial institutions to monitor ATM machine usage on campus.

CAMERA PLACEMENT:
The following guidelines apply to the placement of cameras on campus:

1. University Police may establish temporary or permanent cameras in public areas of the campus. These cameras will not make audio recordings.
2. This policy does not apply to covert cameras used by University Police for criminal surveillance as governed by New York Penal Law.
3. Cameras may not be established in private areas of the campus without obtaining a warrant and only subject to Section 2 above. Private areas include residence hall rooms, bathrooms, shower areas, locker and changing rooms, areas where a reasonable person might change clothes, and private offices. Additionally, rooms for medical, physical, or mental therapy or treatment are private. Private areas also include the entrances, exits, lobbies, exam rooms or hallways of the Beard Wellness Center. The only exceptions are cameras used narrowly to protect money, documents, supplies or pharmaceuticals from theft, destruction, or tampering.
4. Cameras shall not be directed or zoomed into the windows of any private residential space or office. To the maximum extent possible, electronic shielding will be placed in the camera so that the camera does not have the capability to look into or through windows.

5. Cameras shall not be directed or zoomed into the windows of any private building not on College property.

NOTIFICATION OF THE CAMPUS COMMUNITY:
This policy shall be available to all students, faculty, staff, and visitors upon request and shall be printed in the annual safety report required by the *Clery Act* and other appropriate publications.

CAMERA USE AND NON-USE:
The following guidelines apply to camera use and non-use:

1. Cameras shall be used exclusively for campus safety purposes. The SUNY Cobleskill Institutional Review Board (IRB), which governs research involving human subjects, does not have jurisdiction over recordings by cameras and may not authorize any individual researcher or organization, whether faculty, staff, student or the general public, to use these cameras, or recordings from the cameras, for research purposes.
2. Surveillance cameras will not be used to evaluate employee performance unless a formal investigation results in a determination that a safety issue may exist.
3. Cameras will not be used to monitor individual students, faculty, or staff, except as necessary for a criminal investigation and except as in accordance with the terms of a warrant.
4. Cameras may be used to monitor a student or employee work area, such as an area with financial transactions or significant safety issues, even if there is only one student, faculty, or staff member employed in that work area. Cameras used to monitor a work area are not intended to view the contents of computer screens. If the cameras can pan to view computer screens, that area will be electronically blurred so that these cameras are not used to monitor employee computer use.
5. The College will not use cameras to prosecute violations, including parking rules, unless review of a formal complaint results in a determination that a campus safety issue exists.

ESTABLISHMENT OF CAMERAS ON CAMPUS:
Temporary cameras are defined as cameras that are established by the University Police to provide additional security for a campus event or situation and that are not in place for more than 30 days. Permanent cameras are established as part of the campus infrastructure and require planning and approval by the appropriate authorities.

The *Clery Act* requires higher education institutions to give timely warnings of crimes that represent a threat to the safety of students or employees, and to make public their campus security policies. It also requires that crime data are collected, reported and disseminated to the campus community and are also submitted to the Education Department. The *Act* is intended to provide students and their families, as higher education consumers, with accurate, complete and timely information about safety on campus so that they can make informed decisions.

The Chief of University Police in consultation with the Personal Safety Committee, the Work Place Violence Advisory Group, and the College President, shall determine placement and use of cameras. Other departments, committees or individuals may recommend placement of cameras.

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

- Protection of buildings and property.
- Building perimeter, entrances and exits, lobbies and corridors, elevators, receiving docks, special storage areas, laboratories, cashier locations, etc.

- Monitoring and recording of access control systems.
- Monitoring and recording restricted access transactions at entrances to buildings and other areas.
- Verification of security alarms.
- Intrusion alarms, exit door controls, hold-up alarms, etc.
- Electronic patrol of public areas.
- Transit stops, parking lots, public (enclosed and unenclosed) streets, farm and animal care areas, shopping areas, vehicle intersections, etc.
- Criminal investigation.
- Robbery, burglary, and theft surveillance.
- Protection of pedestrians.
- Monitoring of pedestrian and vehicle traffic and vehicles in traffic areas at intersections.

CAMERA MONITORING:
Images and recordings may only be monitored by University Police Officers, staff with responsibility for residence hall security, persons responsible for adjudication of campus code of conduct violations, and other officials as authorized by the President of the College. No students may be hired to monitor recordings or images. Staff responsible for installation and maintenance of surveillance equipment may access recordings only to the extent necessary to carry out their duties.

If the University Police**,** in consultation with the President**,** believes it is necessary to aid in an investigation or search, short recordings or image stills may be released to the media or the public. Prior to releasing the recordings or images, the face and identifying features of all those persons not of interest to the investigation will be blurred.

Those officers and authorized staff approved for monitoring will receive training in effective, legal and ethical use of the monitoring equipment. These officers and authorized staff will receive a copy of this policy and provide written acknowledgement that they have read and understand this policy. Officers and authorized staff will receive any and all updates or amendments to this policy.

STORAGE MEDIA:
Recordings will be stored in a manner consistent with available technology and transported in a manner that preserves security. Current and archived recordings shall be kept locked and secured. Current and archived recordings under review by authorized officials shall be subject to a process where the recordings are signed in and out in a logbook.

Recordings not related to or used for an investigation will be kept strictly confidential and destroyed within 120 days. Recordings or images used for investigation or prosecution of a crime shall be retained until the end of the court or judicial proceedings and appeal period unless directed otherwise by a court.

No attempt shall ever be made to alter any recording. Editing or otherwise altering recordings or still images, except to enhance quality for investigative purposes or blur features as described above, is strictly prohibited.

Transmission of recordings using the internet or campus network will use encryption technology to ensure that recordings are not improperly accessed. University Police will work with the

Information Technology Services staff to establish security for the system and to ensure proper password and encryption technology for recordings or images transferred or transmitted over the internet or on the campus network.

DESTRUCTION OR TAMPERING WITH CAMERAS:
Any person who tampers with or destroys a camera or any part of the electronic surveillance system may be prosecuted in the criminal justice system as well as the campus judicial system.

Approved July 2011