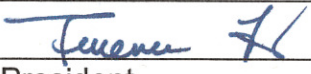


## BBCC ADMINISTRATIVE PROCESS

<b>Title:</b> SECURITY SURVEILLANCE CAMERAS	<b>AP 7706</b>	<b>Implementing Board Policy:</b> 7700
<b>Originating Department:</b> Safety & Security	<b>Originated:</b> 12/2014	<b>Effective Date:</b> 2/23/15
<b>Previous Revisions:</b>	<b>Approved:</b>  President	

### 1.0 Purpose

- 1.1 The purpose of this policy is to regulate the use of camera systems used to observe and record public areas for the purposes of safety and security.
- 1.2 Big Bend Community College (BBCC) 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 and safety camera systems. The surveillance of public areas is intended to deter crime, loss prevention, general risk management and assist in protecting the safety of the BBCC community. This policy addresses the college's safety and security needs while respecting and preserving individual privacy.
- 1.3 This procedure is to formalize procedures for the installation of surveillance equipment and the handling, viewing, retention, dissemination, and destruction of surveillance records to ensure the protection of individual privacy rights in accordance with BBCC's core values and state and federal laws.
- 1.4 The existence of this policy does not imply or guarantee that cameras will be monitored in real time 24 hours a day, seven days a week.

### 2.0 Authority/References

- 2.1 Implementing Board Policy 7700.
- 2.2 International Association of Campus Law Enforcement Administrators (IACLEA) accreditation standard 12.2.2 "Video Surveillance."
- 2.3 RCW 9.73.030 addresses the ability of individuals and agencies of the State of Washington to conduct surveillance. This procedure provides that it is unlawful to intercept or record any private conversation by any device electronic or otherwise designed to record or transmit such conversations regardless of how the device is powered without first obtaining the consent of all the parties engaged in the conversation.
  - 2.3.1 BBCC complies with this code by refusing to install any security camera that has audio recording capabilities.
- 2.4 Electronic Communications Privacy Act of 1986 prohibits the interception of any wire, oral or electronic communication and only permits the recording of communications where the parties have given prior consent.
  - 2.4.1 BBCC complies with this act by refusing to install any security camera that has audio recording capabilities.
- 2.5 U.S. Constitution, Amendment IV and Washington State Constitution both provide in pertinent part that no person shall be disturbed in his or her private affairs, or his or her home invaded,

without authority of law. The decision to install video surveillance cameras must take into consideration this "right to privacy."

- 2.5.1 BBCC complies with these constitutional amendments/sections by refusing to install a video camera system in any area where a person has a reasonable expectation of privacy at the time of taping. This is further advanced by installing systems so that only open and public areas are under surveillance. In such areas there is no reasonable expectation of privacy. The goal is to balance the individual's right to privacy with BBCC's need to supervise, control, and efficiently operate our facilities.

### **3.0 Duties of BBCC Campus Security and Big Bend Technology**

- 3.1 BBCC Campus Safety in conjunction with Big Bend Technology (BBT) has the authority to select, coordinate, operate, manage, and monitor all campus security surveillance systems pursuant to this policy.
- 3.2 All departments using camera surveillance are required to coordinate surveillance operations through Campus Safety and BBT and comply with this policy in their respective operations.
- 3.3 BBT and Campus Safety are responsible for advising departments on appropriate applications of surveillance technologies and for providing technical assistance to departments preparing proposals for the purchase and installation of security camera systems. These offices shall monitor developments in the law and in security industry practices and technology to ensure that camera surveillance is consistent with the best practices and complies with all federal and state laws. BBT and Campus Safety will review any complaints regarding the utilization of surveillance camera systems and determine whether this policy is being followed.

### **4.0 Scope**

- 4.1 This policy applies to all personnel and departments of BBCC in the use of security cameras and their video monitoring and recording systems.

### **5.0 Process for Requesting Installation of a Security Camera**

- 5.1 Individual colleges, departments, programs, or campus organizations installing video surveillance equipment shall submit a written request to their appropriate dean or vice president describing the proposed location of surveillance devices, justifying the proposed installation, providing a cost estimate, and identifying the funding source or sources for purchase and ongoing maintenance.
- 5.2 The appropriate dean or vice president will review the request and recommend it to Campus Safety and BBT, if appropriate. These two groups will be responsible for reviewing and approving or denying all proposals for security camera equipment.
- 5.3 BBT shall oversee the installation of all approved security camera systems with the assistance of the Campus Safety, as required.

### **6.0 Placement of Cameras**

- 6.1 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.
- 6.2 No audio shall be recorded.
- 6.3 Camera positions and views of residential housing shall be limited. The view of a residential housing facility must not violate the standard of a reasonable expectation of privacy.
- 6.4 Monitoring by security cameras in the following locations is prohibited:

- 6.4.1 Restrooms
  - 6.4.2 Student dormitory rooms in the residence halls
  - 6.4.3 Locker rooms
  - 6.4.4 Classrooms not used as a lab
- 6.5 The installation of “dummy” cameras that do not operate is not allowed.
- 6.6 All installed video cameras shall be visible.
- 6.7 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, guest or employee.

## **7.0 Access and Monitoring**

- 7.1 All recording or monitoring of activities of individuals or groups by college security cameras will be conducted in a manner consistent with college policies, state and federal laws, and will not be based on the subjects’ personal characteristics, including age, color, disability, gender, national origin, race, religion, sexual orientation, or other protected characteristics.
- 7.2 Furthermore, all recording or monitoring will be conducted in a professional, ethical, and legal manner.
- 7.3 All personnel with access to college security cameras should be trained in the effective, legal, and ethical use of monitoring equipment.
- 7.4 Camera control operators shall be trained in the technical, legal, and ethical parameters of appropriate camera use.
- 7.5 Camera control operators shall receive a copy of this policy and provide written acknowledgment that they have read and understood its contents.
- 7.6 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 President or designee.
- 7.7 When an incident is reported, the personnel responsible for the area in question may request Campus Safety to review the images from the camera. As circumstances require, the President may authorize others to review images. A record log will be kept of all instances of access to, and use of, recorded material.

## **8.0 Appropriate Use and Confidentiality**

- 8.1 Personnel are prohibited from using or disseminating information acquired from college security cameras, except for official purposes.
- 8.2 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 President or designee.
- 8.3 Personnel are expected to know and follow this policy. If personnel violate this policy, the employee may be disciplined up to termination of employment.

## **9.0 Exceptions**

- 9.1 This policy does not apply to cameras used for academic purposes. Cameras that are used for research, communications, class projects or the like would be governed by other policies involving human subjects and are, therefore, excluded from this policy.
- 9.2 This policy does not address the use of student/employee personal cameras, Webcams, video recording events, or live streaming for general use by the college.

9.3 This policy 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 video recording of athletic events for post-game review, video recording of concerts, plays, and lectures, live stream activity or video recorded interviews of persons. Automated teller machines (ATMs), which may utilize cameras, are also exempt from this policy.

## **10.0 Storage, Retention, and Release of Recordings**

10.1 No attempt shall be made to alter any part of any surveillance recording.

10.2 Surveillance centers and monitors will be configured to prevent camera operators from tampering with or duplicating recorded information.

10.3 All surveillance records shall be stored in a secure location for a period of 30 calendar 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 Director of Campus Safety or the President.

10.3.1 Any image(s) that have been determined to have investigative value and is downloaded for retention beyond 30 calendar days will be sealed, logged, and stored in such a manner that it protects its custody and evidential integrity. Security will take possession and maintain such evidence to ensure chain-of-custody and confidentiality.

10.4 Individual departments shall not store video surveillance recordings.

10.5 At BBCC, images of students collected by the College's surveillance system are considered "law enforcement unit records" under the *Family Educational Rights and Privacy Act* (FERPA). Accordingly, the College may disclose information from law enforcement unit records to anyone, including outside law enforcement authorities, without the student's consent. See 34 CFR § 99.8. The captured imagery is collected on a server separate from educational records.

10.6 The Public Records Officer will review all external requests to release records obtained through security camera surveillance. The college may seek consultation and advice from the assigned Assistant State Attorney General as needed related to these requests prior to the release of any records outside of the college. In most instances, only those persons with legitimate educational, law enforcement or security purpose may view video.

10.7 A log shall be maintained of all instances of access to or use of surveillance records.

10.7.1 The log shall include the date and identification of the person or persons to whom access was granted.

10.7.2 The log will also indicate the footage as a Law Enforcement Unit Record.