AP 3535 Public Safety Camera System

References:

Constitution of the United States 4 Am.; California Constitution Declaration of Rights Article I, Section 1; Searches and Seizures Article I, Section 13; Government Code 6250-6270; Penal Code 627-627.10, 632; New Jersey v. T.L.O., 485 U.S. 325 (1989)

1. **DEFINITION**

The Santa Clarita Community College District ("District") operates a public safety camera system ("System"), which is comprised of digital cameras operating without audio. One exception is the cameras at the Early Childhood Education Center(s) used for academic purposes which record video and transmit live audio: such System cameras will be operated pursuant to written releases and consent agreements. The System may produce video recordings, without audio, or still photos ("Images"). The District shall not access cameras embedded in District-issued equipment without the permission of the employee.

2. PURPOSE AND SCOPE

The purpose of the System is to create a safer environment for all students, employees, visitors and guests.

The System will be implemented in locations where it is determined that its use will enhance the security and safety of either individuals or property without violating the reasonable expectation of privacy as defined by law. The System may or may not be monitored in real time, therefore individuals should not expect that System Images captured by the cameras are contemporaneously monitored by the District.

The System can be used to deter and/or detect crime or misconduct, to help safeguard against potential threats to the public, and to help manage emergency response situations during natural and man-made disasters. Public safety cameras may be used in conjunction with campus access control and two-way communications to enhance access to buildings and emergency notification.

The District may install cameras, in compliance with the law, if there is a need for an investigation arising from the "reasonable suspicion" of a violation of the law, Board Policy, or Administrative Procedures. In no case will cameras be used by a supervisor to monitor employee compliance with regular daily job responsibilities. Any cameras installed for investigative purposes shall comply with the law and not be placed in Private Spaces. Images from cameras installed for employee investigations may only be accessed for viewing under the authority of the Vice-President, Human Resources and Campus Safety Management.

3. DELEGATION

The implementation of this procedure will be delegated based on the subject matter. The CEO may designate the individual(s) required to implement this procedure and/or perform the necessary duties reference herein. Those individuals will receive the applicable legal and regulatory training to perform those duties. The "Designee" shall be defined based on the area of responsibility, as listed below:

- Vice-President, Human Resources
- Vice-President, Student Services
- Vice-President, Business Services
- Vice-President, Technology

- **District Employee Matters**
 - Campus Safety & Student Matters
- 3rd Party Liability Matters
- **Technological Support**

(Installation, maintenance and camera support)

4. CAMERA LOCATIONS AND EXCLUSIONS

<u>Camera Location Plan & Inventory</u>: The CEO or designee shall be responsible for reviewing and approving or denying all aspects of the System, including installation of new cameras, adjusting or removing existing cameras, administration, and operation. Information Technology, in coordination as appropriate with Human Resources, Student Services, Risk Management, Campus Safety, or Facilities, will prepare and present a plan identifying the appropriate locations of each camera for approval by the CEO or designee. Information Technology will maintain a master inventory of all existing and approved public safety cameras.

<u>Private Space</u>: The District will not place cameras in **any** areas where there is a "reasonable expectation of privacy" as defined by law including but not limited to bathrooms, locker rooms, private offices, shared offices, changing rooms and other areas where a person may reasonably expect to change clothes with the expectation of privacy. Additionally, areas dedicated to medical, physical, or mental therapy or treatment are private areas for the purpose of this policy. Furthermore, System cameras will not be used in classrooms without the prior consent of the faculty member and the CEO or designee (Education Code 78907).

<u>Public Space</u>: The System will be implemented in public locations where it is determined that its use will enhance the security and safety of either of either individuals or property.

Cameras may generally be used in hallways, lobbies, stairwells, parking lots, fields, gymnasiums, stadiums, common areas, cafeterias, auditoriums/theatres, loading docks, indoor and outdoor assembly areas, building exteriors and outdoor public areas, points of public ingress and egress that are located within areas owned or controlled, via leases or other contractual arrangements, by the District.

<u>High Value Locations</u>: The District reserves the right to use the System to monitor legitimate business concerns including but not limited to storage areas for supplies and equipment, or cash handling areas. Employees assigned to such spaces will be notified that System cameras are installed in these locations. System cameras placed in high value location will be used, to the extent possible, narrowly to protect persons, money, real or personal property, documents, supplies, equipment, or pharmaceuticals/chemicals from theft, destruction, or tampering.

5. NOTIFICATION OF CAMERA SURVEILLANCE

Except for cameras used for public safety investigatory purposes, the District shall provide reasonable written notice to the public, visitors, employees, and students by posting signage at entrances to District locations or other high traffic exterior areas that a System has been

installed indicating that the area may be monitored or recorded. The signage will also inform individuals that the "premises are protected by video surveillance and cameras are recording, but not continually monitored". Signs shall be installed in reasonably lit and visible locations. The District reserves the right to conduct confidential investigations that may require the use of cameras without providing notice; such surveillance will be limited in duration to meet a specific objective, and will not be used in a Private Space.

6. RECORDING AND VIEWING

System Images will be recorded and stored on a 24-hour basis every day of the week. Recordings not otherwise needed for official reasons shall be retained for a period of not less than six (6) months and thereafter shall be erased. Any recordings, including involving litigation, violation of District regulations or needed as evidence in a criminal or civil proceeding, shall be retained by Information Technology on original storage medium until the issue has been resolved. (Government Code 34090.6)

When activity warranting further investigation is reported or detected at any camera location, Campus Safety officers or a Designee may selectively view the appropriate camera live stream or recording and relay any available information, as relevant, to Law Enforcement, a Risk Management Administrator, a Human Resources Administrator or a Student Services Administrator. If, during the course of viewing the camera live stream or recording, an employee is identified as being involved in an incident, Designee will immediately alert the Vice-President, Human Resources. Use of System Images in employee discipline shall be implemented with the guidance of the applicable collective bargaining agreement and in accordance with applicable law.

System Images obtained by the District may be viewed by authorized District management personnel or Campus Safety officers as necessary. The CEO or Designee shall review and approve or deny requests for individuals to have access and viewing privileges of System Images. Employees at the District will be authorized to operate the System or view System Images if they meet the following:

- possess a legitimate business need for access consistent with the purposes of the District's policies and procedures, including but not limited to, criminal, legal, health, or safety concerns;
- are appropriately trained and supervised in the technical, responsible, legal, and ethical use of the public safety cameras; and,
- sign a written acknowledgement that they have read, understood, and will comply with the District's policies and procedures.

The District may rely on the System Images in connection with the enforcement of District policies, administrative procedures, and other applicable law including but not limited to student and employee disciplinary proceedings, matters referred to local law enforcement agencies, or in litigation or other proceeding involving person(s) whose activities are shown on the System Images and relate to the proceeding. System Images may become part of a student's educational

record or an employee's personnel record in accordance with applicable law, AP 7145 – Personnel Files, and collective bargaining agreements

System Images may be used for a variety of purposes, including administrative and criminal investigations and monitoring of activity around high value or high threat areas.

7. PROHIBITED ACTIVITY

<u>No Audio Recording</u>: Under no circumstances shall the District's System be equipped to record audio or other sound(s). Any audio capability in District's System shall be permanently deactivated prior to use by the District. Furthermore, audio shall not be part of any System recordings made, reviewed or stored by the District, except with two-party consent.

8. STUDENT OR PERSONNEL RECORDS

To the extent System Images create student records or personnel records, the District shall comply with all applicable state and federal laws related to record maintenance, retention and disclosure including the Family Educational Rights and Privacy Act ("FERPA"), the California Public Records Act and applicable student records and personnel file sections of the California Education Code, AP 7145 – Personnel Records, as well as relevant provisions from existing collective bargaining agreements (20 USCA 1 23 Education Code 49060-49079, 44031; Government Code 6250-6270).

9. RELEASE OF SYSTEM IMAGES, INCLUDING THROUGH A CALIFORNIA PUBLIC RECORDS ACT REQUEST

If the District receives a request for the release of recorded System Images under the California Public Records Act, such requests will be submitted to the Public Information Office per BP/AP 3300 Public Records Act Request. The Vice-President, Public Information, in consultation with and authorization from the respective Vice-President and District legal counsel, will review each request and determine whether to release the recordings, or whether the System Images are legally exempt from release by law, including under the California Public Records Act, as discussed in more detail below.

Requests for recorded System Images from other entities or via court order, subpoena, or other legal process shall be promptly submitted to the CEO or designee to allow the District to consult with the District's legal counsel as needed. Every reasonable effort will be made to preserve the data requested pending the review and response by the District's legal counsel.

System Images that are requested by the public or media will be made available only to the extent required by law. All requests for real-time System Images, review of recorded video footage, and/or copies of recorded video footage will generally be evaluated in accordance with the following guidelines:

	Request by Public or Media	Request by Entities or Law Enforcement Agencies
Request to Observe	Restricted and not subject to	Will be evaluated on a case-by-
Real Time System	requirements set forth by the	case basis subject to applicable

Images	California Public Records Act.	law
Request to View Stored System Images and/or for Copies of Stored System Images	Will be evaluated subject to requirements set forth by the California Public Records Act.	Will be evaluated subject to requirements set forth by the California Public Records Act, and/or pursuant to federal; and state law.

The District may withhold the requested System Images if the public's interest in disclosure is outweighed by the public's interest in non-disclosure, including certain instances when releasing the System Images would compromise a police investigation.

The District will provide assistance to persons making California Public Records Act requests as required by law, and may fill in and submit Request for Release of Recorded Images Form if the person does not wish to do so. Although preferable, the form need not be fully completed in order to initiate the request. The District shall respond to all requests for System Image review and copies of System Images in the timeframes required by applicable laws and regulations.

The District reserves the right to assess fees for the actual costs of copies, including CDs, DVDs, or other media devices.

10. ANNUAL REVIEW OF THE SYSTEM

Information Technology will conduct an annual review of the System. The review will include an inventory of cameras and the date of installation. The review may include processes and records pertaining to the System and to confirm the System has been operated and maintained in compliance with District policies and procedures. The results of each inventory or audit will be maintained by the Information Technology Administrator, and will be reported to the CEO's office.

Annually, a presentation will be made by the Vice-President, Human Resources and the Vice-President, Business Services to the Workplace Safety Committee regarding the number and types of incidents on campus and the location.

Per the respective collective bargaining agreement, COCFA and CSEA "will receive notice of the number and location of video recording devices to be used on campus. This will be updated each year as devices are added." In conjunction with the Workplace Safety Committee, feedback may be provided and additional information shared.

CPC Approved: December 1, 2020

Board Review Date: December 16, 2020

Next Review Date: Fall, 2026