CAMPUS SECURITY

The Superintendent or designee shall ensure that campus security procedures are developed which are consistent with the goals and objectives of the District's comprehensive safety plan and site-level safety plans.

(cf. 0450 - Comprehensive Safety Plan)

These procedures shall include strategies and methods to:

1. Secure the campus perimeter and school facilities in order to prevent criminal activity. These strategies shall include an analysis of the building security system, lighting system, and campus fencing. Procedures to ensure unobstructed views and eliminate blind spots caused by doorways and landscaping shall also be considered. In addition, parking lot design may be studied, including methods to discourage through traffic.

2. Secure buildings from outsiders and discourage trespassing. These procedures may include requiring visitor registration, requiring staff and student identification tags, and patrolling places used for congregating and loitering.

   (cf. 1250 - Visitors/Outsiders)
   (cf. 3515.2 - Disruptions)
   (cf. 5112.5 - Open/Closed Campus)

3. Discourage vandalism and graffiti. These methods may include plans to immediately cover graffiti as well as campus beautification projects and shall also include students and the community in these projects.

   (cf. 3515.4 - Recovery for Property Loss or Damage)
   (cf. 5131.5 - Vandalism, Theft and Graffiti)

4. Control access to keys and other school inventory.

   (cf. 3440 - Inventories)

5. Detect and intervene with school crime. These procedures may include the creation of a school watch program, an anonymous crime reporting system, analysis of school crime incidents, and collaboration and communication with local law enforcement agencies.

CAMPUS SECURITY

All staff shall receive training in building and grounds security procedures.

(cf. 3515.3 - District Police Department)
(cf. 4131 - Staff Development)
(cf. 4231 - Staff Development)
(cf. 4331 - Staff Development)

These procedures shall be regularly reviewed and updated in order to reflect changed circumstances and to assess progress in achieving safe school objectives.

Keys

All keys used in a school shall be the responsibility of the principal or designee. Keys shall be issued only to those employees who regularly need a key in order to carry out normal activities of their position.

The person issued a key shall be responsible for its safekeeping. If a key is lost, the person responsible shall report the loss to the principal or designee immediately and shall pay for a replacement key and re-keying expense.

Keys shall be used only by authorized employees and shall never be loaned to students.

The master key shall not be loaned and the duplication of school keys is prohibited.

Surveillance Equipment

Authorized users of the surveillance television camera system shall be appointed/approved by the Superintendent or designee. The Superintendent or designee shall maintain a list of all District employees with authorized access to the surveillance control and recording center and to any stored recording media.

Authorized users shall receive training regarding proper use of the surveillance television equipment, rules regulating privacy and District policy. Authorized users shall be trained in the technical use of the surveillance television cameras and how to use the controls to maximize efficiency and clarity of focus. Included in such training shall be maintenance, storage and use/release of surveillance images, changing recording media and record keeping. Authorized users shall restrict the use of the system to that for which it is intended, property conservation.

Although constant, real-time monitoring may not always be possible, the District and the individual school site(s) shall make every effort to ensure that video images are monitored on a scheduled basis. Monitoring shall take place at the school site in the area designated

as the monitoring center. The monitoring center should be in an enclosed area not subject to unauthorized access or casual entry.

Information obtained through video surveillance shall be used exclusively for security and law enforcement purposes. The use of the surveillance television system for the purpose of monitoring personal safety issues, gathering evidence for use in internal employment or labor-related investigations, gang association, or other non-property related purposes is prohibited. Viewing areas on campus (classrooms, bathrooms, locker rooms), off campus, into neighboring property, into vehicles or onto any areas where there is an expectation of privacy is also prohibited. No sound is to be monitored or recorded in connection with the surveillance television system.

Remote surveillance television monitoring may also be conducted via intranet, internet, wireless or other means. Any system of remote monitoring shall ensure the security of the surveillance television system and must include a system utilizing passwords or other identifiers to gain access. Remote monitoring shall only be conducted by the Superintendent and authorized designees.

Expansion of existing surveillance television systems shall include like equipment and technology and shall be installed within the perimeter coverage guidelines outlined in this policy. Equipment used in expanding surveillance television systems shall not be located where it is easily defeated or damaged.

All surveillance television systems throughout the District shall include like equipment and technology. All campus-based surveillance television systems shall be able to be upgraded to permit remote site monitoring by internet capable computers utilizing a host site or other means to receive uploaded real-time camera images from each site and providing selective access to those images by authorized users. Although monitoring may be done remotely, the school site shall maintain access control over the surveillance television tapes.

Surveillance television system(s) used in the District shall be capable of being upgraded to utilize wireless internet technology to monitor real-time images or hand-held digital communication devices. The surveillance television system shall also be capable of being upgraded to include motion-activated alarms. In connection with an alarm system that is activated when an individual crosses a surveillance television camera's field of view, wireless monitoring may permit District personnel to increase the effectiveness of an investigation.

Any expansion of the current surveillance television system(s) may be conducted by an approved surveillance television system vendor selected under the guidelines of the District's bidding policies for contracted work.

CAMPUS SECURITY

Only a qualified surveillance television vendor shall maintain repair, clean, service, adjust or replace any surveillance television equipment or components during the warranty period.

Any unauthorized maintenance, repair or modification of the surveillance television camera hardware or related devices by District employees or unqualified vendors may void system warranties. Only the installing surveillance television vendor should perform service on the surveillance television system during the warranty period.

Operating system software shall not be altered, downloaded, copied, edited or modified by anyone other than a qualified surveillance television vendor. Corrupted software resulting from tampering may void the system warranties.

Repair, replacement or alteration of District-installed connective cables, conduit, power supply or other infrastructure may be performed by District in coordination with the surveillance television vendor to ensure such action is not disruptive or damaging to the system.

Any defect in system operation shall be reported both verbally and in writing to the surveillance television vendor as soon as possible to ensure that any guarantees or warranties are maintained in force. All physical damage to the surveillance television system shall be documented and investigated.

A surveillance television system log shall be maintained at each site, which records each system user, dates and times of use, activity, repairs or notices of malfunction. Such system logs shall be maintained on an ongoing basis and kept available in secure storage for no less than three years. System logs older than three years should thereafter be archived in accordance with District policy.

The school District shall utilize digital technology in the surveillance television system(s) deployed. Video images shall be recorded onto DAT-type magnetic tapes or other appropriate medium and secured at the school site in a fire resistant cabinet. Recorded video images stored on media shall be maintained for a period of no less than one year from the date which the image was recorded or for a longer period if required by the District's internal record keeping procedures.

The Superintendent or designee shall approve requests for access to recorded and stored video images. Recorded surveillance television images are only to be viewed by authorized personnel. The Superintendent or designee may authorize viewing of recorded surveillance television images in the event of an ongoing law enforcement investigation, an incident involving property damage or loss, or for other reasons the Superintendent may deem appropriate.

CAMPUS SECURITY

All surveillance television recording media removed from the school site shall be signed out by the Superintendent or designee. When returned, the recording media shall be signed back in by the same person. All surveillance television recording media shall be considered legal evidence and treated as confidential or as directed by Counsel. Release of original surveillance television media to individuals or agencies outside of the District may only occur when a subpoena or the court order is received and reviewed by District Counsel.

Original surveillance television media shall never be edited or manipulated in any manner. When recorded surveillance television media is requested by any law enforcement agency as part of an ongoing investigation, a duplicate may be provided for that purpose upon approval by District Counsel. The original surveillance television recording media shall be protected from accidental overwrite or erasure during the duplicating process.

A periodic audit of random images from the stored surveillance television recording media shall be conducted to ensure that the surveillance television cameras have not been moved or altered and that the images captured by the system are not inclusive of areas prohibited by this policy and where campus users may have an expectation of privacy.

Prior to the operation of the surveillance system, the Superintendent or designee shall ensure that signs are posted at conspicuous locations (entrances) at each affected school site and grounds. These signs shall inform students, staff and campus visitors that surveillance cameras are in use for the protection of property.

Legal Reference:

EDUCATION CODE
32020 Access gates
32211 Threatened disruption or interference with classes
35294-35294.9 School safety plans
38000-38005 Security patrols
PENAL CODE
469 Unauthorized making, duplicating or possession of key to public building
626-626.10 Disruption of schools

Management Resources:
CDE PUBLICATIONS
Safe Schools: A Planning Guide for Action, 1995
CSBA PUBLICATIONS
Protecting Our Schools: Board of Education Strategies to Combat School Violence, 1995

Regulation **BREA OLINDA UNIFIED SCHOOL DISTRICT**
Approved: June 25, 2001 Brea, California
Revised: June 8, 2009