BUSINESS AND NONINSTRUCTIONAL OPERATIONS

Campus Security

The Superintendent or designee shall develop a campus security plan which contributes a positive school climate, fosters social and emotional learning and student well-being, and includes strategies to:

1. Secure the campus perimeter and school facilities in order to prevent criminal activity

   These strategies include a risk management analysis of each campus' security system, lighting system, and 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 strategies may include installing locks, requiring visitor registration, providing staff and student identification tags, and patrolling of places used for congregating and loitering.

3. Secure the district's network infrastructure and web applications from cyberattacks

   These strategies may include performing an independent security assessment of the district's network infrastructure and selected web applications.

4. Discourage vandalism and graffiti

   These strategies may include plans to immediately cover graffiti and implement campus beautification.

5. Control access to keys and other school inventory

6. Detect and intervene with school crime

   These strategies may include the creation of a school watch program, increasing adult presence and supervision, establishing an anonymous crime reporting system, monitoring suspicious and/or threatening digital content, analyzing school crime incidents, and collaboration with local law enforcement agencies, including providing for law enforcement presence.

7. Additionally, all staff shall be made aware of their responsibilities regarding the immediate reporting of potential homicidal acts to law enforcement, and receive training in the assessment and reporting of such threats.

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

Use of Video Equipment

1. Administration will determine placement of cameras ensuring their placement is restricted identifiable, i.e. visible cameras (not covered) and within the common areas of the school or any other district facilities

2. Areas chosen for cameras will include locations where placement will serve as a viable deterrent (such as hallways and high incident and traffic areas)

3. Cameras may also be placed on District buses.

4. Cameras will not be placed where individuals have a reasonable expectation of privacy (e.g. change rooms, restroom interiors, the nurse's office, etc.).

5. Security system signage will be posted at each of the sites and on school buses where security cameras are in use.

6. Students and parents will be notified each year of the existence of District security cameras through publications.

7. No inoperable "dummy" cameras will be installed without specific cause and prior Superintendent/Designee approval.

Personnel Access

1. Campus Access

    a. School Principal or Designee - full access

    b. School Resource Officer (Fresno Police Department SRO / Fresno Sheriff’s Department) - full access

2. District Access

    a. Superintendent or Designee - full access

    b. Assistant Superintendents - full access

    c. Area Administrators - full access

    d. Director of Maintenance, Operations, Transportation (MOT) or Designee - full access for purposes of maintenance and site support

    e. Director of Information Technology or Designee - full access for purposes of maintenance and site support

Protection of Information and Disclosure

The District shall treat the video recording of an individual student as part of that student's educational record. Only video that is exported from the video recording system related to a specific incident can be made part of a student record.

The District will comply with all applicable State and Federal laws and District Board policies related to record maintenance, retention, and disclosure. All video is stored temporarily in the recording device and is not archived or backed up.

Requests to review video recordings shall comply with all State and Federal laws and Board policies relating to student records and guidelines for responding to public requests for information.

1. All requests for review of video recordings that are considered an educational record or personnel record will be made as follows:

    a. All viewing requests must be submitted in writing. Requests for viewing will be limited to those parents/guardians, students and/or district officials with a direct interest in potential disciplinary issues as authorized by the responsible administrator. Only the portion of the video recording related to the specific incident will be made available for viewing.

    b. Approval/denial for viewing will be made within a reasonable amount of time of receipt of the request and communicated to the requesting individual, relative to the severity of the incident.

    c. A written notation will be recorded in the student information system of the date and time of the viewing of a student recording, the reason for the viewing and the person present at the time of the viewing.

    d. Video recordings will remain the property of the District and may be reproduced only in accordance with the law and applicable Board policy.

2. Storage and Security

    a. Storage of video recordings will be dependent upon the type of system installed, which could vary from site to site and with the introduction of new technology. Records storage will adhere to applicable Board policy and California Education code.

    b. Video recordings held for review of property, staff or students incidents will be maintained in their original form pending resolution. Recordings will then be released for deletion, copied for authorized law enforcement agencies, or retained as required in accordance with established District procedures and applicable law.

c. All recordings or other storage devices that are not in use should be stored securely and in a controlled access area. Access to the storage devices shall be limited to authorized personnel only.

d. Security recordings are presumed exempt from disclosure under the California Public Records Act.

Locks

All state-funded new construction and modernization projects shall include locks that allow doors to classrooms and any room with an occupancy of five or more persons to be locked from the inside. Student restrooms and doors that lock from the outside at all times are not required to have locks that can be locked from the inside. (Education Code 17075.50, 17583; 24 CCR 1010.2, 1010.2.8.2)

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 job responsibilities.

The principal or designee shall create a key control system with a record of each key assigned and room(s) or building(s) which the key opens.

Keys shall never be loaned to students, parents/guardians, or volunteers, nor shall the master key ever be loaned.

The person issued a key shall be responsible for its safekeeping. The duplication of school keys is prohibited. If a key is lost, the person responsible shall immediately report the loss to the principal or designee and shall pay for a replacement key.

Regulation approved: 4/9/02
Regulation revised: 11/27/07; 1/30/2023; 2/17/23