

MODESTO CITY SCHOOLS

Administrative Regulation

AR 3515

BUSINESS AND NONINSTRUCTIONAL OPERATIONS

Campus Security

The Superintendent or designee shall develop a campus security plan which contributes to 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 and interior spaces from outsiders and discourage trespassing

These strategies may include installing locks, requiring visitor registration, providing staff and student identification tags, and patrolling 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

BUSINESS AND NONINSTRUCTIONAL OPERATIONS

Campus Security

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

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.

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

The principal or designee shall be responsible for all keys used in a school. Keys shall be issued only to authorized 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.

Any 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.

BUSINESS AND NONINSTRUCTIONAL OPERATIONS

Campus Security

Surveillance Systems

The intent of the security camera system deployed by Modesto City Schools is to protect the safety and security of students, employees and authorized visitors to school and administrative sites and to safeguard District facilities and equipment from theft and vandalism.

Locations Subject to Monitoring

Security cameras may be used to monitor buildings, exterior campus areas, including but not limited to: parking lots, perimeters, entrance and exit doors, interior and exterior hallways, picnic areas, foyers, pools, lobbies, stairs, elevators, gymnasiums, athletic fields, cafeterias, stadiums and large open interior spaces.

Security cameras will not be installed in classrooms or offices without the prior authorization of the Superintendent/designee. (Education Code 51512)

Notice and Authorization to Monitor

Prior to use of security camera systems, the District shall notify students, parents/legal guardians and staff that surveillance may occur, the location(s) of the surveillance, and the purpose for/use of the security camera footage, in accordance with Board policy, administrative regulations, other District safety protocols and applicable laws.

Whenever and wherever permanent security cameras are installed, signs will be posted at conspicuous locations informing people that the buildings and grounds may be under video monitoring

System Operation

1. Security cameras will be installed both inside and outside of buildings in areas around school campuses and other District-owned facilities as directed by the safety planning committee and when storage capacity for security camera recordings is available that meets the established District's procedures.
2. Access of any security cameras can only be made by an authorized security camera system user.

BUSINESS AND NONINSTRUCTIONAL OPERATIONS

Campus Security

3. No interior covert security cameras will be installed without specific cause and prior Superintendent/designee approval.
4. No “dummy” security cameras or empty decoy security camera domes will be deployed on any District-owned property. All installed equipment will be active and connected to the security camera system. Security cameras may be offline due to technical issues, maintenance, hardware failures or reconfiguration.
5. The security camera system shall not monitor areas where the public, students or employees have a reasonable expectation of privacy. Examples include, but are not limited to: locker rooms and restrooms.
6. There will be no intentional security video monitoring or recording of any lawful union activity on District property. This excludes any gatherings that take place in the field of view of existing security cameras.
7. The use of the security camera system shall be supervised and managed by the Information and Technology Services Department. The use of security cameras will be supervised and managed by the Maintenance and Operations Department.
8. Security video recording should be reviewed when there is a need to do so, either because an incident has been reported or is suspected to have occurred.

Examples include, but are not limited to: incidents of property damage, theft, trespassing, personal injury or any unlawful activity.

9. Administrative staff assigned to the security camera system and security cameras will be required to review and apply these regulations in performing their duties and functions related to the operation of the system and security cameras.
10. Students are prohibited from unauthorized use, tampering, or otherwise interfering with security video recording and/or security camera system equipment. Discipline for such action will be based on the Student Conduct Code.

BUSINESS AND NONINSTRUCTIONAL OPERATIONS

Campus Security

11. Staff is prohibited from unauthorized use, tampering, or otherwise interfering with security video recording and/or security camera system equipment. Violation of this policy may result in disciplinary action.
12. Staff is prohibited from the use of personal and/or non-District security camera equipment on District property. Violation of this policy may result in disciplinary action.
13. The District shall provide reasonable safeguards, which may include, but are not limited to, password protection on the security cameras and the security camera system, managed firewalls, and control of physical access to protect the security camera system from unauthorized users or unauthorized use.
14. These regulations shall be incorporated into any training and orientation programs. The regulations should be reviewed and updated periodically.
15. Authorized users for the security camera system shall not view live or recorded video from the security cameras that would enable general public viewing.
16. Security camera equipment shall be used in accordance with all District Board policies, including the District's non-discrimination

Storage and Security

1. Storage of security video recordings will be dependent upon the type of system installed and with the introduction of new technology. There is no maximum storage time defined by this policy.
2. Security video recordings held for review of property, staff or student incidents will be maintained in their original form pending resolution. Recordings will then be released for deletion, copied for student records, copied for staff records, copied for authorized law enforcement agencies, or retained as required in accordance with established District procedures and applicable law.
3. All security video 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 should be possible only by authorized personnel. Logs shall be kept of

BUSINESS AND NONINSTRUCTIONAL OPERATIONS

Campus Security

all access to recordings.

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

Student Records

1. The District shall treat the security video recording of an individual student as part of that student's educational record. Only video that is exported from the security video recording system related to a specific incident can be made part of a student record.
2. The District will comply with all applicable State and Federal laws and District Board policies related to record maintenance, retention, and disclosure. All security video is stored temporarily in the recording device and is not archived or backed up.
3. Requests to review security video recordings shall comply with all applicable State and Federal laws and Board policies relating to student records and guidelines for responding to public requests for information.

Viewing Requests

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

1. 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 site administrator. Only the portion of the security video recording related to the specific incident will be made available for viewing.
2. 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.
3. A written log will be maintained for those viewing security video recordings,

BUSINESS AND NONINSTRUCTIONAL OPERATIONS

Campus Security

including the date and time of the viewing, reason for viewing, date the recording was made of the incident, location of the camera that made the recording, and signature of the viewer.

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

Legal Reference:

EDUCATION CODE

17070.10-17079.30 Leroy F. Greene School Facilities Act

17583 Classroom security locks; modernization projects

32020 Access gates

32211 Threatened disruption or interference with classes 32280-

32288 32289.5 School safety plans

35160 Authority of governing boards

35160.1 Broad authority of school districts

35266 Reporting of cyber attacks

38000-38005 Security patrols

49050-49051 Searches by school employees

49060-49079 Student records

49390-49395 Homicide threats

PENAL CODE

469 Unauthorized making, duplicating or possession of key to public building 626-

626.10 Disruption of schools

626-626.11 Weapons on school grounds and other school crimes

CALIFORNIA CONSTITUTION

Article 1, Section 28(c) Right to Safe Schools

UNITED STATES CODE, TITLE 6

665k Federal Clearinghouse on School Safety Evidence-Based Practices

UNITED STATES CODE, TITLE 20

1232g Family Educational Rights and Privacy Act

CODE OF REGULATIONS, TITLE 24

1010.2 Door operations

1010.2.8.2 Lockable doors from the inside

CODE OF FEDERAL REGULATIONS, TITLE 34

99.3 Definition of education records

GOVERNMENT CODE

11549.3 Independent security assessment

Management Resources:

ATTORNEY GENERAL OPINIONS

83 Ops.Cal.Atty.Gen. 257 (2000)

75 Ops.Cal.Atty.Gen. 155 (1992)

BUSINESS AND NONINSTRUCTIONAL OPERATIONS

Campus Security

Management Resources (cont.):

CALIFORNIA DEPARTMENT OF EDUCATION PUBLICATION

Safe Schools: A Planning Guide for Action Workbook, 2002

NATIONAL INSTITUTE OF JUSTICE PUBLICATION

The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies, 1999

US DOE PUBLICATION

FAQs on Photos and Videos under FERPA

COURT DECISIONS

Brannum v. Overton County School Board (2008) 516 F 3d 489

New Jersey v. T.L.O. (1985) 469 U.S. 325

CSBA PUBLICATIONS

Protecting Our Schools: Governing Board Strategies to Combat School Violence, 1999

WEBSITES

CSBA: <http://www.csba.org>

California Department of Education, Safe Schools Office: <http://www.cde.ca.gov/ls/ss>

National Institute of Justice: <http://www.ojp.usdoj.gov/nij>

California Military Department: <https://calguard.ca.gov/>

U.S. Department of Homeland Security, Fusion Centers: <https://www.dhs.gov/fusion-centers>

California State Threat Assessment System: <https://calstas.org/>

CSBA District and County Office of Education Legal Services: <https://legalservices.csba.org/>

U.S. Department of Education, Protecting Student Privacy: <https://studentprivacy.ed.gov/>

National School Safety Center: <http://www.schoolsafety.us/>

Cross References (cf.):

0450 – Comprehensive Safety Plan

1250 – Visitors/Outsiders

1330.1 – Joint Use Agreements (N/A)

3000 – Concepts And Roles (N/A)

3440 – Inventories

3515.2 – Disruptions

3515.3 – District Police/Security Department

3515.31 – School Resource Officers (N/A)

3515.4 – Recovery For Property Loss Or Damage

3515.5 – Sex Offender Notification (N/A)

3515.7 – Firearms On School Grounds (N/A)

3516 – Emergencies And Disaster Preparedness Plan

3516.2 – Bomb Threats

3530 – Risk Management/Insurance

4112.6 – Personnel Files

4119.1/4219.1/4319.1 – Civil And Legal Rights (N/A)

4119.1/4219.1/4319. – Whistleblower Protection

4131/4231/4331 – Staff Development

4158/4258/4358 – Employee Safety (N/A)

5112.5 – Open/Closed Campus

BUSINESS AND NONINSTRUCTIONAL OPERATIONS

Campus Security

Cross References (cf.)(cont.):

5116.2 – Involuntary Student Transfers
5125 – Student Records
5125.1 – Release Of Directory Information
5131.1 – Bus Conduct
5131.2 – Bullying
5131.5 – Vandalism And Graffiti
5131.7 – Weapons and Dangerous Instruments
5137 – Positive School Climate
5138 – Conflict Resolution/Peer Mediation (N/A)
5138 – Electronic Signaling or communication Devices
5141.52 – Suicide Prevention
5142 – Safety (N/A)
5144 – Discipline (N/A)
5144 – Subpoena Power, Expulsion Proceedings
5144.1 – Suspension And Expulsion/Due Process
5145.12 – Search And Seizure
5145.9 – Hate-Motivated Behavior
6142.4 – Service Learning/Community Service Classes (N/A)
6164.2 – Guidance/Counseling
6184 – Continuation Education
7111 – Evaluating Existing Buildings (N/A)
7111 – School Sites Superintendent’s Responsibility
9321 – Closed Session

REVIEWED: April 20, 2009
May 22, 2017
April 1, 2023