



# Use of Security Cameras and Surveillance in Schools Best Practices

<b><u>Recommendations</u></b>	<b>2</b>
<b><u>Policy</u></b>	<b>3</b>
<b><u>Applicable Regulations</u></b>	<b>4</b>
<b><u>Disclosures</u></b>	<b>7</b>
<b><u>Access to Recordings</u></b>	<b>8</b>

## Recommendations

1. All Districts should establish a formal Board Policy regarding the use of recording and surveillance devices on district property to ensure the health, welfare and safety of all staff, students and visitors to District property, and to safeguard district facilities and equipment.
2. District administrators and staff should be aware of privacy limitations regarding the use of such equipment and seek the advice of counsel whenever questions arise.
3. The District should post surveillance signage at all campus and facility entrances disclosing the use of surveillance equipment on the premises.
4. The District should also notify staff and students through newsletters and staff handbooks of the on premises surveillance program.
5. Once an event takes place or a request has been made for a recording, take steps to immediately preserve the recording and isolate it from any routine deletion process until a disclosure determination is made and be sure to keep a disclosure copy for future reference.

# Policy for Use of Security Cameras and Video Surveillance

As a component of school safety and risk management, every District should have a clearly established policy on the use of security cameras and video and audio surveillance on school property. The policy should effectively address privacy issues and provide fair disclosure to students, staff and visitors that on-campus surveillance measures are in place. The policy, at a minimum, should:

- Authorize the use of video camera surveillance on District property to monitor the health, welfare, and safety of all staff, students and visitors to District property, and to safeguard District facilities and equipment. Video cameras may be placed in locations as deemed appropriate by the appropriate designated school administrators.
- Notify staff and students through student/parent and staff handbooks and signage that on-campus video and audio surveillance may occur on District property and on vehicles used for District-provided transportation.
- Notify students or staff in violation of Board policies, administrative regulations, building rules, or law that images, video and audio captured through surveillance may be used as evidence that may subject them to appropriate disciplinary and legal action, including, but not limited to, disclosure to law enforcement.
- State that video recordings may become a part of a student's educational record or a staff member's personnel record. The District shall comply with all applicable state and federal laws related to record maintenance and retention. Generally, data retention in California Districts should be one year. See <https://oag.ca.gov/system/files/opinions/pdfs/02-207.pdf>.

The District's policy should include reasonable procedures intended to preserve data related to a known incident which involves injury to students, staff or members of the public or property, or which involves any potential violation of the law or District policies, procedures, or rules of conduct. For example, in the event of any accident involving injury to persons or loss of property, a copy the video surveillance recording should be placed in any accident report files maintained pursuant to the District's policy regarding the preparation of school accident reports. (See ASCIP's "A Guide to Reporting School Accidents" for further information regarding maintaining documents and information pertaining to School Accidents).

# Privacy Laws and Security Camera Placement

As in all matter involving issues of privacy, each District should always consult with their legal counsel as specific issues arise. In addition, it is possible that certain staff rights may be part of an employee bargaining agreement or MOU, which should be consulted. In general, school officials may observe and record what they lawfully can see with the naked eye. The Fourth Amendment protects people, not places. Activities occurring in parking lots, hallways, classrooms, auditoriums and other open areas usually do not involve reasonable expectations of privacy. For faculty and staff, the guidelines in the area of the Fourth Amendment come from the U.S. Supreme Court. The Court has ruled that the expectation of privacy is "reasonable" when: (1) a person acts as though he or she has a subjective expectation of privacy, and (2) the courts agree that the expectation in a specific context is reasonable. See *California v. Ciraolo*, 476 U.S. 207 (1986). When this standard is applied in the school employee setting, a reasonable expectation of privacy exists in those areas that have been given over to an employee use such as an office, room or cubicle reserved for that individual's exclusive use. This would usually *exclude* break rooms, school buses and common areas.<sup>1</sup>

The California Constitution contains an explicit guarantee of privacy in Article I, Section 1 of its Declaration of Rights. Courts have applied this protection to the workplace, schools and the state government. For this right to be upheld, video surveillance must fulfill three criteria:

- 1) It must **not** constitute an intrusion.
- 2) It must **not** intrude in a location or context where there is a reasonable expectation of privacy.
- 3) It must **not** outweigh other interests by the gravity of the alleged violation.

The same general rules that govern video cameras apply to audio recordings. California makes it a *crime* to record or eavesdrop on any confidential communication, including a private conversation or telephone call, without the consent of all parties to the conversation. (Cal. Penal Code § 632). The statute applies to "confidential communications" -- i.e., conversations in which one of the parties has an objectively reasonable expectation that no one is listening in or overhearing the conversation.

Accordingly, appropriate video and audio recording device placement is very important. The table set forth below are provided as a guideline regarding acceptable security video and audio device placement. Again, all of these selections should go through an administrative vetting process.

---

<sup>1</sup> See, Video Surveillance: The Right To Privacy & Safe Schools By Bernard James, Professor of Constitutional Law, Pepperdine University, Summer 2010 edition of the NASRO Journal of School Safety. <https://nasro.org/cms/wp-content/uploads/2015/09/Video-Surveillance-The-Right-To-Privacy-and-Safe-Schools.pdf>

**TABLE 1- Appropriate Locations for Camera Placement**

**Likely, Acceptable Security Camera Placement**

Location	Functional Reason	Potential Use as Evidence	Costs/Risks
Main entrance/public administrative office areas	Records all visitors' entry and exit	Recordkeeping; security	Initial installation; maintenance; monitoring
All building exits	Records all exits from buildings; reduces truancy	Recordkeeping; explains inconsistencies with main office entry/exit balance	Initial installation; maintenance; monitoring
Near lockers, trophy cases, bookcases, storage areas	Records locker use; records activity near personal property; reduces theft	Recordkeeping; security	Initial installation; maintenance; monitoring
On buses	Records activity during rides; records passenger entry and exit; reduces unruly behavior	Recordkeeping; records vehicle accidents	Initial installation; maintenance; monitoring
Parking lots	Records suspicious activity; reduces thefts	Records accidents; security; recordkeeping	Initial installation; maintenance; monitoring
Playgrounds, athletic fields, and cafeterias	Reduces unruly behavior; records accidents	Records accidents; security; recordkeeping	Initial installation; maintenance; monitoring

**Less Common, but Acceptable Security Camera Placement**

Location	Functional Reason	Potential Use as Evidence	Costs/Risks
Hallways	Records all student movements; reduces unruly behavior	Recordkeeping; security	Initial installation; maintenance; monitoring; privacy concerns
Classrooms	Records classroom activities; reduces abuse and molestation claims	Recordkeeping; security	Initial installation; maintenance; monitoring; privacy concerns; collective bargaining agreements

**TABLE 1 (CONT) – Appropriate Locations for Camera Placement**

**Unlikely, Unacceptable Security Camera Placement**

Location	Functional Reason	Potential Use as Evidence	Costs/Risks
Restrooms	Records all visitors' entry and exit	Recordkeeping; security	Initial installation; maintenance; monitoring; <u>extreme privacy concerns</u>
Athletic locker rooms or other rooms wherein clothes may be changed	Records all exits from buildings; reduces truancy	Recordkeeping; explains inconsistencies with main office entry/exit balance	Initial installation; maintenance; monitoring; <u>extreme privacy concerns</u>
Staff Offices	Records Office Activity	Recordkeeping; security	Initial installation; maintenance; monitoring; <u>extreme privacy concerns</u> ; collective bargaining agreements

# **SURVEILLANCE DISCLOSURES**

As discussed above, In order to prevent a person from raising the defense of some general expectation of privacy on the school campus, it is also an important practice to post signage at all school entrance locations disclosing the existence of surveillance on campus. Sample language includes:

## **VIDEO SURVEILLANCE ON CAMPUS**

**School district buildings and grounds are equipped with electronic surveillance for the safety of students, staff and visitors. Your actions may be recorded and preserved.**

In addition, it is recommended that the District notify staff and students through student/parent and staff handbooks that video/audio surveillance may occur on campus and throughout District property and that such recordings could be used as evidence against students, staff or visitors in an appropriate disciplinary action or for referral to law enforcement agencies.

# ACCESS TO SURVEILLANCE RECORDINGS

## EMPLOYEE ACCESS

Typically, school surveillance equipment is maintained by District IT department personnel. Password protected access to the information should initially be limited to specific school staff, including IT, security personnel, school resources officers (SRO's), safety/risk managers and top administrators. The data should not be generally available to all staff and certainly not to the public through web sites. Upon knowledge of an event, authorized staff shall direct access to and preserve all data in a "hold" status.

The District should distribute, collect, and maintain "Video Surveillance Use Guidelines for Employees" for all employees involved in the video surveillance process. Specific District staff should be designated to 1) issue passwords to employees who are authorized to access to school video surveillance viewing, 2) install the necessary software for viewing on administrative computers, and 3) train administrators on the usage of video surveillance software.

All District personnel who have been provided with access the District's video recordings, including principals, and any other District administrators and technical personnel pertinent to the implementation of the video surveillance procedures should sign the "Video Surveillance Use Guidelines for Employees."

## REQUESTS FOR ACCESS BY THIRD PARTIES OR ENTITIES

Requests for copies of any audio or video surveillance recording received by the District from any person or entity (including current or former District employees) who has not been authorized by the school principal to access to such recordings, should be *immediately* forwarded to the Superintendent or designee. In addition, in the event the recording is part of a routine deletion cycle, immediate steps should be taken to preserve the recording, until disclosure rights are determined. The request may come in the form of a request under the Family Education Rights and Privacy Act (FERPA), civil or criminal subpoena, search warrant, a California Public Records Act (CPRA) request, a request of a current or former employee pursuant to Labor Code Section 1198.5, Court Order, or other form.

As the District may be required by law to provide the requested recording, and there may be restrictions regarding what can and cannot be provided due to student privacy or other legal reasons, the Superintendent or designee should consult with the District's general counsel to determine whether and how to respond to any such request. If, after consultation with the District's general counsel, the Superintendent or designee authorizes a recording to be provided

to the requesting person or entity, the District should ensure that the recording is retained in the Districts files and that *a duplicate of* the recording is delivered to the requesting person or entity.

If personally identifiable information regarding a student is depicted in any recording which requested pursuant to a subpoena or court order, the principal is required by law to make a reasonable effort to notify the parent and the student in advance of compliance with the subpoena or court order, if lawfully possible, within the requirements of the subpoena or court order. (See Education Code section 49077.)

Requests for video or audio surveillance recordings that involve or are related to potential employee misconduct, including those requested by current or former employees or law enforcement, should also be forwarded to the District's Human Resource Department for review. A recording or image of a staff member that may be used in a personnel action is subject to the laws and regulations regarding school personnel actions, including an employee's right to comment on derogatory information placed in his/her file.

## **FERPA**

School-based video surveillance recordings involving students may be considered education records protected by Education Code 49061 and the Family Education Rights and Privacy Act (FERPA), 20 U.S.C. 1232f – 1232i and F.S. 1002.22. FERPA affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of information from the records. FERPA requires that the school comply with a parent's request for access to the student's records within 45 days of the receipt of a request. Generally, a school is required to provide copies of education records to a parent if the failure to do so would prevent the parent from exercising the right to inspect and review the records.

## **SUBPOENAS**

A subpoena is a formal court order requiring the attendance of a person at court to give evidence, to produce documents or to do both. If served with a subpoena, the person to whom the subpoena is directed must comply with it unless otherwise excused by the party issuing the subpoena. Generally, when a person is served with a subpoena to produce documents, a sum of money (conduct money) should also be tendered by the party issuing the subpoena to cover the costs of assembling the requested materials and sending them to the court. If insufficient money has been provided to cover these costs, the District should still comply with the subpoena.