SCHOOLS LEGAL SERVICE

LAW UPDATE
SPECIAL EDUCATION

PHONE: (661) 636-4830 • FAX: (661) 636-4843
E-mail: sls@kern.org • www.schoolslegalservice.org

October 2021

ELECTRONIC DEVICE USE AND MONITORING IN THE VIRTUAL ENVIRONMENT

California regulates the ability of government agencies, including school districts, to search and record information on or from electronic devices (e.g., computers and cell phones) in a way that extends beyond federal law requirements. While many district staff are familiar with these regulations, virtual classrooms have brought about an increased dependency on the electronic devices needed to support them and some new implications of some old rules.

SB 178 for example places limits on the district's ability to search electronic devices that extend beyond the standard search and seizure rules applicable to students. Although districts may ordinarily conduct a search when there are reasonable grounds to suspect the search will turn up evidence of wrongdoing and the search is not excessively intrusive, SB 178 removes that right for searches of electronic device information.

Except in emergencies or when a device is believed to be lost, SB 178 prevents districts from accessing information on any electronic device without a warrant or "the specific consent of the *authorized possessor* of the device."[1] "Authorized possessor" is defined narrowly to mean "the possessor of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device."[2] In other words, consent may only be given by one who is both in possession of the device and either owns the device or has the owner's permission to possess it.

Aside from removing the district's ability to search an electronic device based on reasonable suspicion, SB 178's narrow authorization seems to prevent parents from remotely authorizing the search of a parent-owned, student-possessed device without the student's permission. In such a situation, districts should have parents authorize the district's seizure and possession of the device before granting consent to search. While this may seem like a distinction without a difference, the legislature found the dichotomy important enough to devote significant portions of the statute to it. Districts, therefore, should be mindful of it.

SB 178 may also limit a district's ability to remotely access information on its own devices when those devices, such as Chrome Books, are lent to students. Although subsection (k) of Penal Code section 1546.1 creates an exception for devices lent to school employees, no similar provision exists for students.

> "(k) This chapter shall not be construed to alter the authority of a government entity that owns an electronic device to compel an employee who is authorized to possess the device to return the device to the government entity's possession."[3]

[1] Cal. Pen. Code § 1546.1(c) (Emphasis added.)
[2] Cal. Pen. Code § 1546(b)
[3] Cal. Pen. Code § 1546.1(k)

As such, districts should consult with legal counsel before accessing such information remotely.

While most district personnel are generally familiar with the prohibition on classroom recordings, many overlook its application to the virtual learning environment. California Education Code section 51512 prohibits the use of:

> "any electronic listening or recording device in any classroom of the elementary and secondary schools without the prior consent of the teacher **and the principal** of the school given to promote an educational purpose."[4]

Students violating this prohibition are subject to discipline, while non-students are guilty of a misdemeanor. Violations sometimes arise from teachers in a virtual class who, when faced with disruption from an unruly parent or student, attempt to document the event by recording it, but neglect to get permission from the principal beforehand.

Penal Code section 632 imposes more severe penalties for closely related activity. Under that statute, anyone "who, intentionally and without the consent of all parties to a confidential communication, uses an electronic... recording device to eavesdrop upon or record the confidential communication...." is guilty of a misdemeanor or felony (depending on the nature of the violation) and subject to a fine of up to $2,500, imprisonment in a county jail for up to a year or in state prison for up to three years.[5] A "confidential communication" is:

> "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering... or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded."[6]

The statute would apply to all one-on-one phone calls, and many conference calls, as well as virtual meetings depending on the number of participants and the nature of the discussion. It is important to note that the statute would not apply where the meeting participants knew the meeting was recorded. In such meetings, district personnel should take care to announce that the session is being recorded before and after the recording begins to create a record of the fact.

Please do not hesitate to contact us with any questions.

– JAMES D. SIMSON

Education Law Updates are intended to alert clients to developments in legislation, opinions of courts and administrative bodies and related matters. They are not intended as legal advice in any specific situation. Please consult legal counsel as to how the issue presented may affect your particular circumstances.

[4] Cal Ed. Code § 51512. (Emphasis added.)
[5] Penal Code § 632(a).
[6] Penal Code § 632(c).