LEGAL SERVICES
California Teachers Association
1705 Murchison Drive
Burlingame, CA 94010
650-697-1400 • www.cta.org

September 2020

LEGAL ADVICE MEMORANDUM

Privacy Considerations in a Distance Learning Environment

As we begin the 2020-2021 academic year, many districts are engaged in distance learning. Most CTA members have returned to a setting that includes the provision and/or recording of live instruction over Zoom and the use of educational technology platforms. This advisory addresses the privacy rights of members and students that are implicated when classes are online rather than in-person.

What is Distance Learning?

California Education Code section 43500, recently passed as part of SB 98 (the 2020 budget bill), defines distance learning as "instruction in which the pupil and instructor are in different locations and pupils are under the general supervision of a certificated employee of the local educational agency." Distance Learning may include, but is not limited to, the following:

- Interaction, instruction and check-ins through the use of a computer or communications technology;
- Video or audio instruction in which the primary mode of communication between the pupil and certificated employee is online interaction, instructional television, video, telecourses, or other instruction that relies on computer or communications technology; and/or
- The use of print materials incorporating assignments that are the subject of written or oral feedback.

(Cal. Ed. Code §43500).

A distance learning program in California must include various components, such as access for all students to adequate devices; content aligned to grade level standards that is provided at a level substantially equivalent to in-person instruction; and daily live interaction with certificated employees and peers. (Cal. Ed. Code §43503(b)).

Distance learning under sections 43500 and 43503(b) can be synchronous (taking place in real time with instruction and/or interaction with participants) or asynchronous (occurring

without simultaneous interaction with participants). An example of asynchronous instruction is recorded video featuring direct instruction of new content that students can watch on their own time.

Educator Privacy Laws and the Online Environment:

In many districts, educators have been asked to record lessons which can be viewed by students at their convenience. This has given rise to the question of whether such a practice requires the consent of the educator under Education Code section 51512. While section 51512 prohibits eavesdropping and the use of recording devices in a classroom without consent of the educator and principal, section 43503(d)(1) clarifies that consent of the individual educator or principal is **not required** for the adoption or implementation of the use of synchronous or asynchronous video as part of a Distance Learning program. (Cal. Ed. Code §43503(d)(1)). (See SB 820). Accordingly, and depending on the specific terms of the collective bargaining agreement, while districts must bargain over the impacts and effects of a distance learning program that uses recorded lessons, a district need not obtain consent of individual educators before implementing a distance learning program that requires educators to record video lessons for instructional purposes.

The Education Code simultaneously makes clear that aside from a district requiring the use of synchronous or asynchronous video as part of a distance learning program pursuant to section 43503, **no other person** may make any audio, video, or digital recording of a local educational agency's (LEA's) live or synchronous distance learning instruction without the educator's **and** principal's prior consent. (Cal. Ed. Code §43503(d)(2)); see also Cal. Ed. Code §51512; Cal. Penal Code §632.[1] Many district policies and collective bargaining agreements also limit the creation or use of recordings in the educational setting.

School employees should be aware that they generally do not enjoy a personal right of privacy when using the employer's network and equipment. Subject to district policies and any applicable CBA language, the district will have access to an employee's district email and use of applications and programs on district equipment. In addition, employees should use separate personal and district/professional accounts for any digital platforms used at work.

Chapters may wish to consider bargainable issues relating to the use of recordings including, but not limited to, how recordings will be secured and how long they will remain posted. Information regarding bargaining implications, including the mandatory bargaining subject of use of recording for evaluative purposes, can be found in: *CTA Bargaining Advisory: Distance Learning During the COVID-19 Pandemic* (3/16/2020), here, *C4OB Bargaining Advisory: Bargaining a Return to Work During the COVID-19 Pandemic and Difficult Economic Times* (5/22/2020) here, and *Sample Contract/MOU Language: Reopening Schools During the COVID-19 Pandemic* (6/22/2020) here.

[1] If there is an unlawful intrusion into or recording of an online class, particularly followed by an unauthorized publication of that recording, then the wrongdoer(s) might be liable for tort claims that may apply depending on the nature of the violation and the specific facts.

Student Privacy Laws and the Online Environment:

The Federal Family Educational Rights and Privacy Act

The federal Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. §1232g and 34 C.F.R. Part 99) protects the privacy of students' education records and their Personally Identifiable Information (PII), such as a student or family member's name, a student's birth date, birth place, or mother's maiden name, contained in those records. Under FERPA, an educational agency or institution is prohibited from disclosing student education records or the PII contained therein, without prior, written consent from the parent, guardian, or adult student, unless the disclosure meets an exception to FERPA's general consent requirement (like, for example, disclosure under the "directory information" exception[2]). Recording a virtual class for other students to view on their own time is permissible as long as the video does not disclose PII or information from any student's educational record.

Educational records subject to FERPA include photos or videos that are directly related to a particular student, meaning the student is the focus of the video (for example, it shows them being injured or having a health emergency, contains their PII, or depicts an act they are disciplined for), and which the educational agency maintains. This does not include videos where the student is incidentally captured or that show the student participating in school activities open to the public and without a specific focus on any individual. It is likely that an all-day recording of classroom instruction could capture videos directly related to individually-identifiable students and at least portions of video could qualify as an educational record, requiring prior, written consent before disclosure to online service providers or others. Examples that could give rise to a recording being deemed "directly related" to a particular student include:

- When a student gives a presentation during a virtual class, that portion of the video could be deemed "directly related" to that student and cannot be disclosed unless prior written consent is obtained from the parent, guardian or adult student. This prohibition on disclosure may include disclosure to other students (including those who were absent) who might want to watch the recording later. Thus, unless prior consent is obtained, class recordings should be redacted of non-disclosable PII and education records before being distributed to other students or any third parties.
- If something occurs during the recording that gives rise to student discipline or a student medical emergency, that portion of the video could be deemed "directly related" to the impacted student and cannot be disclosed unless prior written consent is obtained from

[2] FERPA defines "directory information" as information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Typically, "directory information" includes information such as name, address, telephone listing, and participation in officially recognized activities and sports. A school may disclose "directory information" to third parties without consent if it has given public notice of the types of information which it has designated as "directory information," the parent's or eligible student's right to restrict the disclosure of such information, and the period of time within which a parent or eligible student has to notify the school in writing that he or she does not want any or all of those types of information designated as "directory information."

the parent, guardian or adult student. As with the prior example, this prohibition on disclosure may include disclosure of the recording to other students, and, unless prior consent was obtained, redactions of non-disclosable PII and education records might be needed before distribution of the recording.

FERPA's prohibition on disclosure of a recording "directly related" to a student does **not** prohibit disclosure to:

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

34 C.F.R. § 99.31.

Also, FERPA does not prevent school officials from identifying and using students' names in class. Thus, the mere appearance and/or use of student names in an online class recording should not raise FERPA concerns so long as the class recording is available only to students enrolled in that class and other authorized individuals.

<u>The Children's Online Privacy Protection Act and Consumer Protection Laws</u>

Under the federal Children's Online Privacy Protection Act (COPPA) (16 CFR Part 312), operators of commercial websites and online services that are directed to children under the age of 13 and that collect, use, or disclose personal information from children, must obtain the consent of a parent or guardian before collecting or using such information.

The California Consumer Privacy Act (CCPA) (Cal. Civ. Code §1798.100 *et seq*.) extends this protection to children up to age 16, and it requires that parents of children under the age of 13 opt in before the child's information is sold, and that *children* age 13-16 opt in before their information is sold. In addition, California's Student Online Personal Information Protection Act (SOPIPA) (Cal. Bus. & Prof. Code §§22584-55), prohibits an operator of an Internet website or online service from knowingly using, disclosing, compiling, or allowing a third party to use, disclose, or compile the personal information of a minor for the purpose of marketing or advertising specified types of products or services.

As LEAs continue to search for alternatives to classroom instruction, they may be tempted to adopt "solutions" from educational technology companies. However, educators and parents/guardians often do not realize that online learning companies collect, store, and sell personal data about the children who register to use these services. Additionally, the

pedagogical effectiveness of many of these new technologies is untested. The “best practices” section below recommends that local unions and educators work with districts to ensure that districts vet and use reliable and secure online educational products.

Best Practices and Considerations:

“Zoombombing”

We have seen reports of people who attempt to gain entry into online classes for the sole purpose of disrupting the learning process. When they enter the class, they may shout inappropriate words, draw pictures on the screen, and sometimes show pornographic images. Some of these individuals even record their attempts and post their successes on YouTube. This conduct is illegal under Education Code sections 51512 and 43503(d)(1), and possibly under California Penal Code section 632, and is punishable with a fine and possible jail time. When districts require educators to provide online lessons as part of a distance learning program, associations should urge districts to do the following to protect student and educator privacy:

- Mandate that all zoom/online calls be password-protected and begin with students being placed into a waiting room so that students can be identified by educators before being permitted to join a class.
- Provide appropriate training so educators will know how to immediately identify unwelcome participants and end calls to stop any harassing or inappropriate behavior.
- Adopt a student and family code of conduct regarding technology use that prohibits the recording and/or use of images and/or sounds contained in online lessons. The policy should make clear that taking photos of any online learning activities is prohibited.
- Counsel educators not to let anyone into a class whom they do not recognize. If “zoombombing” occurs, an educator should immediately and calmly end the session, and request the district’s and chapter’s assistance if needed to address any subsequent distribution of recorded video/images.

Recording of Instruction

If districts require educators to record lessons as part of a distance learning program, associations should also urge districts to:

- Remind students (particularly those in the upper grades) and families that they cannot make audio, video and digital recording of lessons without consent of the educator and principal, and that doing so is prohibited by Education Code sections 51512 and 43503(d)(2), and Cal. Penal Code section 632. As discussed above, adopt a student and family code of conduct that protects privacy, prohibits sharing of district recordings, and promotes responsible digital citizenship.
- Use virtual learning resources with strong privacy settings.
- Avoid having student images appear in recordings, to the extent possible. However, regardless of whether a class is recorded, a district’s policies can permit an educator to

require a student to leave their camera on during online instruction, for purposes of promoting and tracking student engagement. Districts should allow students to choose a distraction-free virtual backdrop to protect their personal privacy.

- If student images do appear in recorded lessons, educators should preview the recording before posting to ensure that no inappropriate content and no impermissible PII or education records are contained in the video. For example, do not include information about specific students, such as their individual grades, in virtual class sessions. If an educator needs assistance in determining which content is not appropriate to disclose (and might need to be redacted), the educator should confer with an administrator.
- Restrict access to posted recordings to students enrolled in that class.

Adopting Education Technology Products

Before adopting new ed tech resources, associations should urge their LEAs to:

- Exercise extreme caution or refrain from signing new contracts with any ed tech company without careful vetting, including vetting for racist or other inappropriate content.
- Ensure that any new ed tech resource complies with COPPA, the CCPA, the SOPIPA, and FERPA.
- Consider whether any ed tech or similar resource used for teletherapy sessions or other medical-related services needs to be HIPAA-compliant.
- Refrain from adopting new ed tech resources if there is no evidence of pedagogical effectiveness.

While LEAs are urged to use a common platform so educators do not have to employ multiple distance learning technologies, educators may also be individually searching for online solutions and resources. Before adopting any new software, technology, app, or online platform, educators should:

- Check any relevant district policies regarding the use of distance learning technologies. In general, only use apps and platforms that are approved by the district.
- Always get parental consent first — send a note home to inform parents about the platform and ask for permission in writing.
- Stick to tools designed with education in mind, especially if students are going to sign up and create accounts.
- Be mindful about how the tools ask students to sign up, enter personal information, or share anything online.
- Educators should not direct students to websites, programs, or social media apps that are not approved by the employer. Avoid apps, games, or websites that seem focused on advertising or that are also aimed at consumers or the business world.

For more information regarding student privacy, see the following documents published by the U.S. Department of Education:
https://studentprivacy.ed.gov/faq/faqs-photos-and-videos-under-ferpa and
https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf