CLASSROOMS IN THE CLOUD

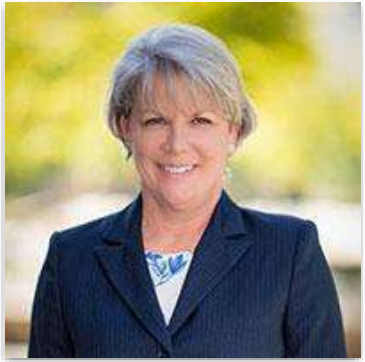
STUDENT PRIVACY & SAFETY DURING THE COVID-19 PANDEMIC

CETPA is now CITE™ CALIFORNIA IT IN EDUCATION

Fagen Friedman & Fulfrost LLP

FUTURE OF PRIVACY FORUM

Speakers



Andrea Bennett
Executive Director,
California IT in Education (CITE)

Amelia Vance
Director of Youth and Education Privacy,
Future of Privacy Forum (FPF)

Gretchen Shipley
Partner,
Fagen Friedman & Fulfrost LLP (F3)

Agenda

1. What are important steps you can take to establish a distance learning program during COVID-19?
2. Is online learning permissible under FERPA?
3. Can I use live video for distance learning? Can I record lessons?
4. What are teachers' responsibilities regarding student misconduct online?
5. Can a teacher sell their online lesson plan?
6. What obligations do schools have under CIPA to filter and monitor school-owned devices or accounts when students are at home?
7. Recommended Resources
8. Q&A

What are important steps you can take to establish a distance learning program during COVID-19?

Tips

- Assess your existing and required resources
- Inquire about accessibility
- Procure what you need
- Develop a flexible educational program
- Identify curriculum

Tips (continued)

- Consider modifications as necessary
- Provide training to staff, parents, and students
- Communicate with your school community
- Guide resource deployment with a process and policies
- Maintain IT Support for staff and students

Is online learning permissible under FERPA?

Considerations

What notice or consent is required before delivering online instruction to students?

Consent must be provided if the tool does not align with FERPA's (or your state law's) requirements.

FUTURE OF PRIVACY FORUM

FERPA

FERPA: The Family Educational Rights and Privacy Act prohibits schools from disclosing PII from students' education records without first obtaining parental consent, subject to certain exceptions. The **"school official" exception** to the consent requirement allows schools to use tools for online learning, so long as the company you are working with:

- Performs an institutional service/function that the school would otherwise use its own employees for;
- Has a legitimate educational interest in the education records/PII;
- Is under the school's direct control re: its use of education records/PII;
- Only uses education records/PII for authorized purposes and doesn't redisclose

What does FERPA require if PII is disclosed to a third party?

- **School Official exception**
  - Annual FERPA notice
  - Direct control
  - Use for authorized purposes only
  - Limitation on re-disclosure
  - Remember parents' right to access their student's education records

The Agora Letter

- Parents cannot be required to waive their FERPA rights as a condition of enrolling in an education program.
- Schools should use the School Official Exception, rather than consent, for the required apps and services.
- Review vendors' Terms of Service closely to ensure that "direct control" has been properly established.

See Letter to Agora for more information:

https://studentprivacy.ed.gov/resources/letter-agora-cyber-charter-school

COPPA

COPPA: The Children's Online Privacy Protection Act applies when children under 13 engage with many online learning tools. COPPA regulates companies and requires verifiable parental consent for the collection, use, or disclosure of PII from children.

If COPPA is implicated, **schools** instead of parents **may provide consent** for the disclosure of PII from children under the age of 13 to a company, if the company uses student information **solely for the benefit of the school**, not for commercial purposes.

> **TIP:** Look for practices like whether a tool uses third-party trackers for advertising purposes which would require parental consent.

Can I use live video for distance learning? Can I record lessons?

Would using video conferencing for online learning violate FERPA?

Schools can use video conferencing tools that meet the **school official exception** to FERPA's consent requirement, discussed earlier.

TIP: Tools developed for general audiences or workplaces were likely not designed with student privacy laws in mind. Before engaging with ANY online platform, **do your due diligence** and ensure appropriate privacy protections are in place. Consider tools developed for learning environments + tools pre-vetted and approved by your school or district.

Considerations

Can educators or administrators post photos or videos of my online class on the internet or social media?

Unlikely without consent. Engaging in online instruction may create an "education record" for a student or students, which is protected from disclosure under FERPA. However, the Department of Education's previous guidance on FERPA and videos has stated that videos only become covered under FERPA when a student is the focus of that video. For example, if online classroom instruction focuses on a particular student, such as the teacher calling on a student to give an answer or a student delivering a book report, the video would become part of the education record for that student, and could not be shared without that student's consent unless a FERPA exception applies.

Considerations

But you can likely share it with the rest of the class. FERPA does not allow students (or their parents) to opt out of data being shared for pedagogical purposes (§ 99.37(c)(1)) (FYI: not an explicit exception to FERPA, so tread carefully). When there is an in-person class, there is sharing of personally identifiable information that is part of education records all the time, from calling on a student (therefore using their name) to knowing which students are in which classes to being able to have students participate in a group project for which they receive a grade. The key for applying this exception is to ask how easy it is to separate out a student's education record. If you can cut a student giving a book report from the recording easily, **and** there was not pedagogical value in that presentation, than you should not post that part of the lesson recording. **However, due diligence must be exercised to guarantee (as much as practicable) that the recording is only accessible to students in that class.**

Considerations

But what about photos?

While videos of online instruction for large groups of students may not create an education record, some students may also have opted out of having their image shared. Posting images or videos of students online that have opted out of having their image shared not only violates that student's privacy, but also could present a dangerous situation. For example, a student who has opted out of having their image shared could have do so because they have a violent non-custodial parent and the student does not want their location identified publicly.

Practice Tip: Verify with District administration whether any students in the class have opted out of having their image disclosed.

FUTURE OF PRIVACY FORUM

TIPS: Have a policy regarding what educators are allowed to do or not do when it comes to using video with students or recording lessons. Encourage teachers to **only record and share the "presentation" part of the lesson, and ensure that the settings for the recording only show the presentation**, not the participant videos or names, or a recording of the "chat box." Ensure that any tool used has appropriate **data retention policies** in place. Consider setting some baseline **rules of engagement** for teachers and students using these platforms. **Be transparent** and let students know that they are being recorded when they are, how long the recording will be stored, who has access to the recording, and think about allowing students to opt-out of attending a live recording.

Best Practices

1. **Define and document the purpose for recording.** Outlining permitted reasons for recording limits needless classroom recordings, and documenting each instance creates an affirmative record for security purposes.
2. **Create guidelines for video storage.** Ensure videos are secure and only available to approved personnel. Create a data retention policy.
3. **Avoid recording classroom discussions with students.**
4. **Remind students and parents that videos are not to be shared,** and are only for educational purposes.
5. **Provide guidance to educators** on how these recordings are stored, shared, and created, including information about how chat transcripts are created.

Adapted from the Consortium for School Networking's "Video Conferencing Tools in the Age of Remote Learning: Privacy Considerations for New Technologies"

FUTURE OF PRIVACY FORUM

Considerations

Does the Presence of Others During Online Instruction Violate Student Privacy Rights?

No. It is not a violation of FERPA for parents and volunteers to observe classrooms at school, and the same rights apply when the classroom instruction is online and videoed from the home. Specifically, under FERPA, the determination of who can observe a virtual classroom, similar to an in-person classroom, is a local school decision as teachers generally do not disclose personally identifiable information from a student's education record during classroom instruction. FERPA neither requires nor prohibits individuals from observing a classroom.

Considerations

Can you record lessons or meetings with students to review for accountability or in case there are later accusations of misconduct?

Probably yes (check your state law), but you cannot share them unless a FERPA exception applies. As discussed, these lessons or meetings likely include PII from an education record, and therefore cannot be shared without consent or unless a FERPA exception applies. Just creating and storing the recording as the school (or an employee acting on behalf of the school) is fine. These recordings would likely be subject to FERPA access rights.

Practice Tip: Store these recordings centrally, and ensure they are deleted in a timely manner. It could be a security risk for individual staff to each have these recordings stored separately on their computers/in accounts.

Considerations

What if My Observations During Online Instruction Lead Me to Reasonably Suspect Neglect or Abuse?

Report it. Teachers are mandated reporters of abuse and neglect regardless of where they see it. The obligation to report to Child Protective Services or Law Enforcement is personal to the teacher. Therefore, while a teacher may want to consult with District administration about any concerns they may have, if the teacher reasonably suspects abuse or neglect, telling the District only is not enough. A teacher's "reasonable belief" may be based on their experience and knowledge in working with children and based on their professional opinion.

Practice Tip: School districts have already seen an uptick in abuse and neglect in the home. As such, staff may want to have a heightened awareness of this issue and refresh their understanding of what is required for mandated reporting.

FUTURE OF PRIVACY FORUM

What are teachers' responsibilities regarding student misconduct online?

Considerations

Teachers have the same responsibility to supervise students as they do in a physical classroom.

Remember your existing policies. Even though online instruction presents new challenges, your existing policies are still in place, including your Code of Conduct and any policies around the responsible use of technology. Consider changing "classroom" settings to create a distraction-free online class environment.

Can a teacher sell their online lesson plan?

Considerations

Lesson plans created to teach students in a given school district technically belong to the school district.

Teachers cannot sell their plans without permission. If a teacher is interested in selling their lesson plan, they should know to first contact the school district for permission.

FUTURE OF PRIVACY FORUM

What obligations do schools have under CIPA to filter and monitor school-owned devices or accounts when students are at home?

Children's Internet Protection Act

CIPA requires schools to create internet safety policies that have:

"[a] technology protection measure that protects against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to use of the computers by minors, harmful to minors. The school must enforce the operation of the technology protection measure during use of its computers with Internet access . . . [t]his Internet safety policy must also include monitoring the online activities of minors."

What are school district's obligations to monitor and filter under CIPA?

The FCC last provided updates on the Children's Internet Protection Act (CIPA) in 2003–unfortunately providing little guidance for monitoring and filtering student's internet access on devices used for distance learning.

CIPA requires schools subject to the law (virtually all public schools) to create internet safety policies that include measures for monitoring, blocking, and filtering both children and adult school computer users from accessing obscenity, child pornography, or other content deemed harmful to minors by the school.

What are school district's obligations to monitor and filter under CIPA?

Schools are operating under different models (some where students take home school-issued devices and others where students use personal devices for distance learning) during this time.

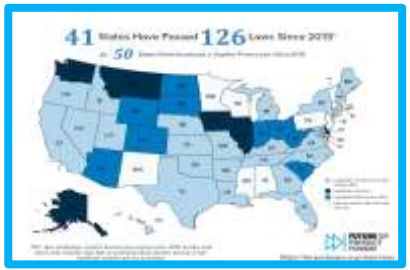
As a best practice, **revisit your schools existing internet safety policies** and model your emergency response after your default policy. Schools across the nation comply with CIPA in a variety of ways–there is no "one size fits all" model. Consider:

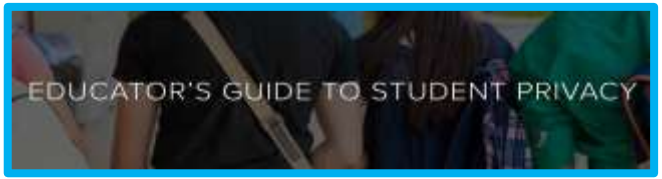
- Limiting monitoring to certain hours of the day;
- Engaging with your school community for feedback; and
- Equity issues that may result from excessive monitoring.

FUTURE OF PRIVACY FORUM

FPF Resources

FERPA | SHERPA

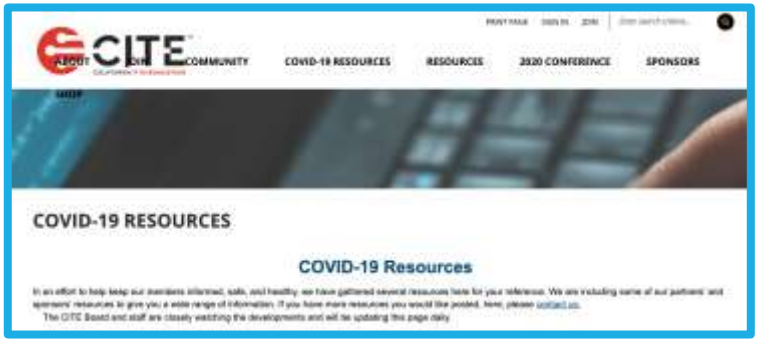


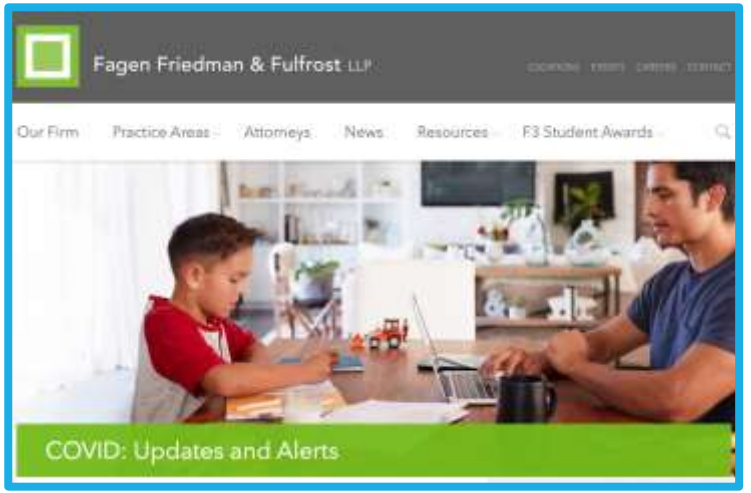


Subscribe to FPF's monthly student privacy newsletter here

For school staff interested in learning more about student privacy, email jpark@fpf.org to join our monthly working group calls.

CITE and F3 Law Resources

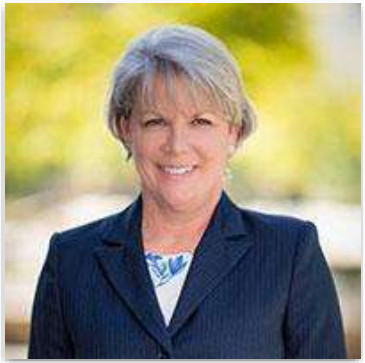




Recommended Resources

- FERPA and Virtual Learning (1-page list of resources), U.S. Department of Education
- FERPA and Virtual Learning webinar slides and recording, U.S. Department of Education
- FERPA and the Coronavirus Disease 2019 FAQ, U.S. Department of Education
- Q&A on Remote Learning and Student Confidentiality, Utah State Board of Education
- Video Conferencing Tools in the Age of Remote Learning: Privacy Considerations for New Technologies, CoSN
- Cybersecurity Considerations in a COVID-19 World, CoSN
- Tips on how educators can avoid COVID-19 cyberattacks, FERPA|Sherpa guest blog by Amy McLaughlin
- Student Privacy and COVID-19 resource, Student Data Privacy Consortium
- Resource on privacy and security for distance learning, Louisiana's SEA
- Zoombombing resources, University of Southern California
- COVID-19 Response: Preparing to Take School Online, CoSN
- Remote learning resources, Connecticut's Commission for Educational Technology

Q&A



Andrea Bennett
Executive Director,
California IT in Education (CITE)

Amelia Vance
Director of Youth and Education Privacy,
Future of Privacy Forum (FPF)

Gretchen Shipley
Partner,
Fagen Friedman & Fulfrost LLP (F3)