FERPA and Zoom Virtual Learning

REGION ONE EDUCATION SERVICE CENTER

OFFICE OF SCHOOL IMPROVEMENT, ACCOUNTABILITY AND COMPLIANCE

Sources

- TEA FERPA & Virtual Learning – April 9, 2020 https://tea.texas.gov/sites/default/files/FERPA%20and%20Virtual%20Learning%204.9.pdf
- Zoom Best Practices for Securing Your Virtual Classroom https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securing-your-virtual-classroom/
- ASCD Educational Leadership Special Report - A New Reality - Getting Remote Learning Right

Current Concerns

Protecting student privacy during remote learning

Cybersecurity breaches (zoombombing & hacking)

FERPA violations

What is FERPA?

The Family Educational Rights and Privacy Act (FERPA) is the federal law that protects the privacy of personally identifiable information (PII) in students' education records.

"Education records" are those records that are:

(1) directly related to a student

(2) maintained by an educational agency or institution or by a party acting for the agency or institution.

FERPA provides parents and eligible students (turned 18 or attending college at any age) the right to protect the PII in students' education records.

An educational agency or institution may not disclose PII from students' education records, without consent, unless the disclosure meets an exception under FERPA. 20 U.S.C. 1232g; 34 C.F.R. Part 99.

TEA FAQ

Does FERPA permit a school district to use video conferencing or other virtual learning software applications to hold classes virtually?

Yes. Educational agencies and institutions may disclose, without consent, education records, or PII contained in those records, to the **providers of such a service or application** under FERPA's "school official" exception. 34 C.F.R. § 99.31(a)(1)(i).

TEA FAQ

Does FERPA provide specific security standards?

FERPA is a privacy rule and does **not** include explicit information regarding security standards. Therefore, school districts should work with their information security officers and attorneys to review information security requirements and terms of service.

TEA FAQ

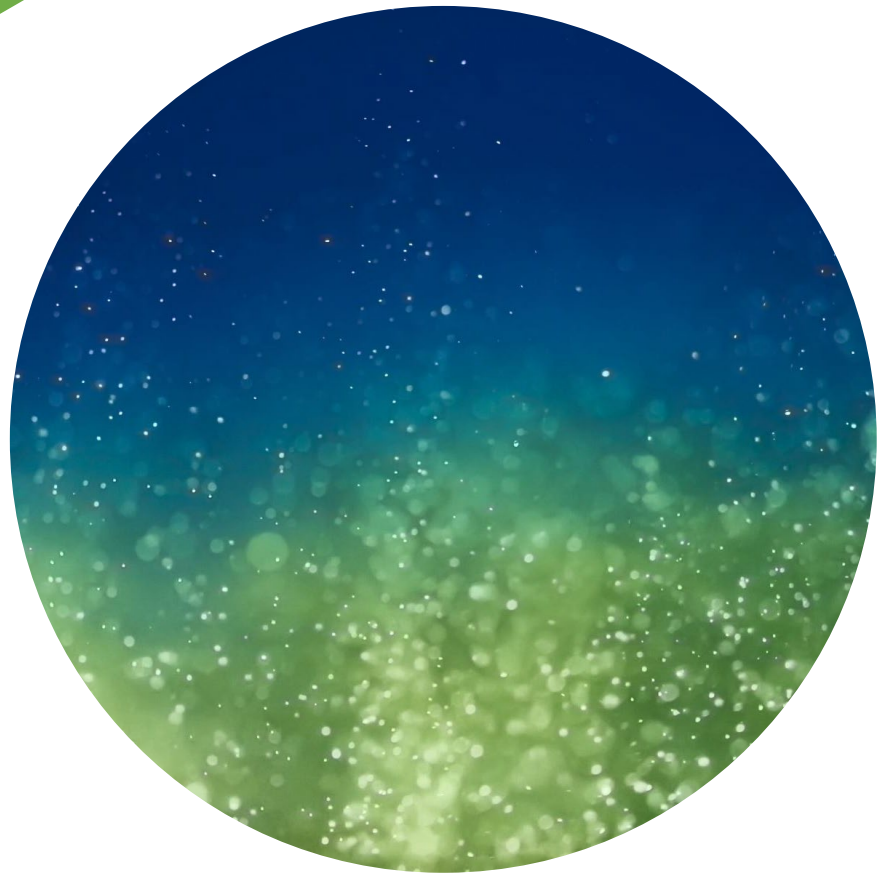
Can <u>non-students</u> observe a virtual lesson?

FERPA applies to the disclosure of tangible records and of information derived from tangible records. A teacher is prohibited from disclosing information from a child's education records to other students in the classroom unless appropriate written consent has been obtained.

Therefore, assuming that during the virtual lesson PII from student education records is not disclosed, FERPA would not prohibit a non-student from observing the virtual lesson.

TEA FAQ

May a teacher record virtual classes and share the recording with students who are unable to attend?



Yes. FERPA does not prohibit a teacher from making a recording of the lesson available to students enrolled in the class, provided the video recording does not disclose PII from student education records during a virtual classroom lesson or appropriate written consent is obtained if PII from the education record is included.

TEA FAQ

I am concerned about managing behavior in my Zoom classroom. What can I do?

Zoom comes pre-stocked with numerous security features designed to control online classrooms, prevent disruption, and help educators effectively teach remotely.

Tips for Zoom: Lock Your Classroom

- You can lock a Zoom session that's already started so that no one else can join.
- It's kind of like closing the classroom door after the bell.
- Give students a few minutes to file in and then click Participants at the bottom of your Zoom window.
- In the Participants pop-up, click the button that says Lock Meeting.
- How to lock your classroom

Tips for Zoom: Control Screen Sharing

- To give instructors more control over what students are seeing and prevent them from sharing random content, Zoom recently updated the default screen-sharing settings for our education users.
- Sharing privileges are now set to “Host Only,” so teachers by default are the only ones who can share content in class.
- However, if students need to share their work with the group, you can allow screen sharing in the host controls.
- Click the arrow next to Share Screen and then Advanced Sharing Options. Under “Who can share?” choose “Only Host” and close the window. You can also change the default sharing option to All Participants in your Zoom settings.
- How to manage screen sharing

Tips for Zoom: Enable the Waiting Room

- The Waiting Room feature is one of the best ways to protect your Zoom virtual classroom and keep out those who aren't supposed to be there.
- *As of March 31, the Waiting Room feature is automatically turned on by default.* You have two options for who hits the Waiting Room before entering a class:
  - All Participants will send everyone to the virtual waiting area, where you can admit them individually or all at once.
  - Guest Participants only allows known students to skip the Waiting Room and join but sends anyone not signed in/part of your school into the virtual waiting area.
- How to enable the Waiting Room

Tips for Zoom: **Lock Down the Chat**

- Teachers can restrict the in-class chat so students cannot privately message other students. We'd recommend controlling chat access in your in-meeting toolbar controls (rather than disabling it altogether) so students can still interact with the teacher as needed.
- How to control chat access

Tips for Zoom: Remove a Participant

- If someone who's not meant to be there somehow manages to join your virtual classroom, you can easily remove them from the Participants menu.
- Hover over their name, and the Remove option (among other options) will appear.
- Click to remove them from your virtual classroom, and they won't be allowed back in.
- How to remove a participant

Other Zoom Security Options

Require registration: This shows you every email address of everyone who signed up to join your class and can help with attendance.

Use a random meeting ID: It's best practice to generate a random meeting ID for your class, so it can't be shared multiple times. This is the better alternative to using your Personal Meeting ID, which is not advised because it's basically an ongoing meeting that's always running.

Password-protect the classroom: Create a password and share with your students via school email so only those intended to join can access a virtual classroom.

Allow only authenticated users to join: Checking this box means only members of your school who are signed into their Zoom account can access this particular class.

Disable join before host: Students cannot join class before the teacher joins and will see a pop-up that says, "The meeting is waiting for the host to join."

Manage annotation: Teachers should disable participant annotation in the screen sharing controls to prevent students from annotating on a shared screen and disrupting class.

Additional Tips from Edsurge

Should teachers record their lessons?

- As mentioned in the earlier guidance from TEA, FERPA does not prohibit a teacher from making a recording of the lesson
- However, some district leaders discourage educators from doing so if children are captured in the video as any images or recordings that include students' faces or names make these materials an "education record"
- Instead, teacher can pre-record their lesson privately and distribute the video afterwards.

Additional Tips from Edsurge

Do not post screenshots of your class online!

- Some enthusiastic teachers and parents eager to show off their Zoom classes online have unwittingly violated student privacy rules.
- Many of these pictures often include not only students' faces—but their full names
- Unless in very specific—and rare—cases where a school and parent has signed off on media agreements authorizing the use of students' name and image, posting such photos online is a violation of FERPA

Additional Tips from ASCD Education Leadership

- Provide information to parents about why you're using the technology and how you're protecting student data privacy
- Give parents the ability to opt their child out of participating in video sessions and have alternative connection methods available

Strategies to Address Current Concerns

Protecting student privacy during remote learning

Cybersecurity breaches (zoombombing & hacking)

FERPA violations

Tammie L. Garcia, Administrator
956-984-6173
tgarcia@esc1.net

Ruben Degollado, Director
956-984-6185
rdegollado@esc1.net

Rosey Guerra, Effective Schools Lead
956-984-6145
rosguerra@esc1.net

Francene Phoenix, Effective Schools Lead
956-984-6027
fphoenix@esc1.net

Aminta Silva, Effective Schools Lead
956-867-8424
amisilva@esc1.net

Intellectual Property Statement

All materials, content, and forms contained in this training/presentation are the intellectual property of the Region One Education Service Center and are intended for use by session participants at the classroom, campus, or district level only. Materials are to be used "as is" without modification.

Materials may not be used for personal benefit or financial gain or for use outside of the school system.