



COVID-19 FAQ: Privacy and FERPA Considerations for Virtual Instruction

April 2, 2020

(512) 463-9000

disasterinfo@tea.texas.gov

tea.texas.gov/coronavirus

General Guidance

- Protections provided by the Federal Educational Rights and Privacy Act (FERPA) apply equally to instruction taking place in a virtual environment as in a brick and mortar facility. Compliance with FERPA does not preclude convening groups made up exclusively of students served by special education in virtual classroom settings.
- LEAs should review contracts and user agreements for software, online programs, and materials used by 3rd party providers to ensure they meet applicable local, state, and federal policies, rules, and laws.
- LEAs should consider creating policy on who has access to virtual and recorded instruction or lessons.
- LEAs should consider selecting tools which allow teachers and educators to create unique access codes as well as functionality to mute the audio and video of participants limiting the potential impact of disruptions or access by outside users.
- LEAs should develop policy and guidance for teachers on the storage, security, and maintenance of recorded instructional video sessions where students were present.

Applicable laws with respect to Online or virtual services and learning

Family Educational Rights and Privacy Act (“FERPA”)[1].

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; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution. FERPA provides parents and eligible students (a student who has turned 18 or is attending college at any age) the right to access a student’s education records, the right to seek to have the records amended, and the right to protect the PII in students’ education records. Under FERPA, an educational agency or institution may not disclose PII from students’ education records, without consent, unless the disclosure meets an exception under FERPA.

An LEA is prohibited from disclosing PII without the written consent of a parent or eligible student, with limited exception.

The “school official” exception permits disclosure of PII to other officials, including teachers, within the LEA whom the LEA has determined to have a “legitimate educational interest.”

- **Take-Away:** The “school official” exception can apply to a 3rd party vendor providing online services if the vendor meets each of the following requirements:
 1. Performs an institutional service or function for which the LEA would otherwise use its own employees;
 2. Has been determined to meet the criteria set forth in the LEA’s annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records;

3. Is under the direct control of the LEA regarding the use and maintenance of education records; and
4. Uses education records only for authorized purposes and may not re-disclose PII from education records to other parties (unless the provider has specific authorization from the LEA to do so and it is otherwise permitted by FERPA).[\[2\]](#)

Protection of Pupil Rights Amendment (“PPRA”)[\[3\]](#). Generally, the PPRA protects students from certain surveys and marketing activities. If such surveying or marketing activities exist, the PPRA requires an LEA to (1) notify parents of the surveying and marketing, (2) give the parents the opportunity to “opt-out” of these activities, and (3) adopt policies, in consultation with parents, addressing these activities.

- **Take-Away:** The PPRA is triggered when certain personal information is collected from the student, so it is important to know what information, if any, is being collected by a 3rd party provider, and if so, what activities that information will be used for. Note: the PPRA does not absolutely prohibit 3rd party providers from distributing generalized, non-targeted advertisements.[\[4\]](#)

Children’s Online Privacy and Protection Act (“COPPA”)[\[5\]](#). Generally, the COPPA requires commercial websites or other online service vendors to first obtain verifiable parental consent prior to collecting personal information from children 13 years of age or younger.

- **Take Away:** The Federal Trade Commission has interpreted COPPA to allow LEAs to consent on behalf of parents in certain, limited circumstances.[\[6\]](#)

General Considerations

Note: “Provider” in this section, means a 3rd party providing the LEA with online services.

- If an online resource or provider utilizes Personally Identifiable Information (PII), meaning the LEA will have to provide student identifying information to the Provider, then the LEA will want to account for privacy.
- If the LEA will be providing PII to the Provider the LEA will want to consider the following:
 - Does the LEA have **written consent** from a parent or eligible student, or
 - Does the Provider qualify under the **school official exception**, or
 - Is there another applicable FERPA exception to written consent?
- If a provider intends to use PII for surveying or marketing purposes, ensure the provider certifies in writing that no violation of the PPRA will occur
- If the Provider will be requesting personal information from students 13 years of age or younger, the LEA should require the Provider to certify in writing that no violation of the COPPA will occur. You may also want to check with your legal counsel to see if your LEA may unilaterally consent on behalf of parents.
- 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.
- Video recordings of virtual classroom lessons qualify as “education records” protected under FERPA only if they directly relate to a student and are maintained by an educational agency or institution or by a party acting on their behalf. FERPA’s nondisclosure provisions may still apply to such video recordings even if they do not qualify as “education records,” if the video recording contains PII from

student education records. Look at current vendor agreements to determine whether video recordings of virtual classroom lessons are or will be maintained as education records beyond the period of instruction, and if so – how, and by whom.

- 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.
- As a best practice, LEAs should discourage non-students from observing a virtual-classroom, similar to the situation with physical classrooms. During the course of classroom instruction, teachers should not be disclosing PII regardless of whether the class is in-person or virtual. 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.
- If a parent or eligible student has requested access to educational records, FERPA requires this information be provided no later than 45 calendar days from the date of the request. This applies to every educational record of a student, regardless of whether the educational record is in the possession of an LEA or its Provider.
- If there is a question or concern regarding HIPAA and the medical information at issue is in the student’s educational record, then FERPA governs and HIPAA does not apply. If you are concerned the medical information is not in an educational record, consult your legal counsel for advice on how to proceed.

Resources

- TEA’s recent webinar, “Cybersecurity Tips and Tools- Cybersecurity Challenges with a Remote Workforce,” has been uploaded and is available at the link below. The Texas Gateway portal is where all of the webinars and cybersecurity resources have been shared for the educational community:
 - <https://www.texasgateway.org/resource/cybersecurity-tips-and-tools>
 - [Questions and Answer Session for Monday March 23rd -- Cybersecurity Challenges Working with a Remote Workforce](#)
 - [K-12 Secure Remote Learning Checklist](#)
 - [Securing Zoom](#)
- [TexasGateway](#) also has a list of questions and considerations for cloud providers.
- USDOE FERPA and Virtual Learning during COVID-19 webinar and presentation materials
 - Webinar: <https://studentprivacy.ed.gov/training/ferpa-and-virtual-learning-during-covid-19-webinar-recording>
 - Presentation materials: <https://studentprivacy.ed.gov/resources/ferpa-and-virtual-learning-during-covid-19>
- [FAQ on student privacy \(FERPA\) and coronavirus](#) from the U.S. Department of Education Student Privacy Policy Office.
- [Q&A on providing services to children with disabilities during the Coronavirus outbreak](#)
- [Best practices guide for Protecting Student privacy while using online education](#)
- [FERPA and Virtual Learning Related Resources](#) from the USDOE Student Privacy Policy Office
- [U.S. Department of Education CoVID-19 Information](#) and Resources for Schools and School Personnel

Legal References and Citations

[1]FERPA at 20 U.S.C. § 1232g; 34 C.F.R. Part 99, Department of Education, “Family Educational Rights and Privacy Act (FERPA)” at <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

[2] Department of Education, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices" at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf

[3] PPRa at 20 U.S.C. § 1232h(c)(2)(C)(i) at <https://law.justia.com/codes/us/2000/title20/chap31/subchapiii/part4/sec1232h>

[4] Department of Education, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices" at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf

[5] COPPA at 16 CFR Part 312 at <https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-312-childrens-online-privacy-protection-rule-safe-1>

[6] Department of Education, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices" at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf

HIPAA at 45 C.F.R. Part 160, Part 162, and Part 164 at <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html>

Department of Health and Human Services, "FERPA and HIPAA" at <https://www.hhs.gov/hipaa/for-professionals/faq/ferpa-and-hipaa/index.html>

Department of Health and Human Services, "Notification of Enforcement Discretion For Telehealth Remote Communications during COVID-19 Nationwide Public Health Emergency" at <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html>

Department of Education, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices" at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf

Department of Education, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices" at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf

Department of Education, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices" at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf

Department of Education, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices" at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf

Department of Education, Letter to Ms. Mamas regarding classroom observations dated 12/2003 at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Letter%20to%20Mamas%28Recreated%29v508.pdf

FERPA at 20 U.S.C. § 1232g; 34 C.F.R. Part 99, Department of Education, "Family Educational Rights and Privacy Act (FERPA)" at <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

Department of Health and Human Services, "FERPA and HIPAA" at <https://www.hhs.gov/hipaa/for-professionals/faq/ferpa-and-hipaa/index.html>