STUDENT PRIVACY POLICY OFFICE
FERPA & Coronavirus Disease 2019 (COVID-19)
Frequently Asked Questions (FAQs)
March 2020

Introduction

The United States (U.S.) Department of Education (Department) is issuing these Frequently Asked Questions (FAQs) regarding the Family Educational Rights and Privacy Act (FERPA) and the coronavirus disease 2019, abbreviated as "COVID-19" and more commonly referred to as "coronavirus."[1] We are working with our Federal partners including the Centers for Disease Control and Prevention (CDC), which is leading the Federal effort to address coronavirus or COVID-19. The U.S. Department of Health and Human Services (HHS) issued on January 31, 2020, a declaration of a Public Health Emergency regarding coronavirus or COVID-19.[2]

The Department's Student Privacy Policy Office (SPPO) prepared this document to assist school officials working with public health officials in managing public health issues related to COVID-19, while protecting the privacy of students' education records. Understanding FERPA helps enable school officials to act quickly and with certainty when confronting challenges that affect the health or safety of students or other individuals.

Educational agencies and institutions, such as school districts, schools, colleges and universities, can play an important role in slowing the spread of COVID-19 in U.S. communities. Through information sharing and coordination with public health departments, educational agencies and institutions can help protect their schools and communities.

The purpose of this document is to assist school officials in protecting student privacy in the context of COVID-19 as they consider the disclosure of personally identifiable information (PII) from student education records to individuals and entities who may not already have access to that information. School officials should work with their State and local public health officials to determine the information needed to address this public health concern. Understanding how, what, and when information can be shared is a critical part of preparedness.

Background

FERPA is a Federal law that protects the privacy of student education records. (20 U.S.C. § 1232g; 34 C.F.R. Part 99) The law applies to all educational agencies and institutions that receive funds under any program administered by the Secretary of Education. The term "educational agencies and institutions" under FERPA generally includes school districts and public schools at the elementary and secondary levels, as well as private and public institutions of postsecondary

---

[1] Please note that this FERPA & Coronavirus Disease 2019 (COVID-19) FAQ document updates the Department's 2009 FERPA & H1N1 document. Other than statutory and regulatory requirements included in the document, the contents of the guidance do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies. This document will be posted at https://studentprivacy.ed.gov and https://www.ed.gov/coronavirus.

[2] HHS declaration posted at https://www.hhs.gov/about/news/2020/01/31/secretary-azar-declares-public-health-emergency-us-2019-novel-coronavirus.html.

education. Private schools at the elementary and secondary levels generally do not receive funds from the Department and are, therefore, not subject to FERPA.

FERPA gives parents certain rights with respect to their children's education records at educational agencies and institutions to which FERPA applies. These rights transfer to the student when he or she reaches the age of 18 or attends an institution of postsecondary education at any age (thereby becoming an "eligible student"). 20 U.S.C. § 1232g(d); 34 C.F.R. § 99.5(a)(1). Under FERPA, a parent or eligible student must provide a signed and dated written consent before an educational agency or institution discloses PII from education records, unless an exception to this general consent requirement applies. 34 C.F.R. § 99.30(a). Exceptions to the general consent requirement are set forth in 20 U.S.C. §§ 1232g(b)(1), (b)(2), (b)(3), (b)(5), (b)(6), (h), (i), and (j) and 34 C.F.R. § 99.31. The term "education records" is defined, with certain exceptions, as 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. 20 U.S.C. § 1232g(a)(4); 34 C.F.R. § 99.3, "Education records." Accordingly, immunization and other health records, as well as records on services provided to students under the Individuals with Disabilities Education Act (IDEA), which are directly related to a student and maintained by an educational agency or institution are "education records" under FERPA.[3] The term "PII" refers to a student's name or identification number, as well as other information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. 34 C.F.R. § 99.3, "Personally identifiable information."

FERPA prohibits educational agencies (e.g., school districts) and institutions (i.e., schools) from disclosing PII from students' education record without the prior written consent of a parent or "eligible student," unless an exception to FERPA's general consent rule applies. 20 U.S.C. §§ 1232g(b)(1) and (b)(2); 34 C.F.R. §§ 99.30 and 99.31. For instance, pursuant to one such exception, the "health or safety emergency" exception, educational agencies and institutions may disclose to a public health agency PII from student education records, without prior written consent in connection with an emergency if the public health agency's knowledge of the information is necessary to protect the health or safety of students or other individuals. 20 U.S.C. § 1232g(b)(1)(I); 34 C.F.R. §§ 99.31(a)(10) and 99.36.

For all other situations where an exception to FERPA's general consent requirement does not apply, educational agencies and institutions must obtain prior written consent of a parent or eligible student to disclose PII from student education records. 20 U.S.C. §§ 1232g(b)(1) and (b)(2); 34 C.F.R. §§ 99.30 and 99.31. We have attached a model consent form at the end of this document. We have also listed the email and contact information for SPPO, the Department office responsible for implementing and enforcing FERPA, if school officials have questions that are not covered in this document.

[3] Parts B and C of the IDEA contain separate privacy regulations that incorporate FERPA provisions and exceptions, including the health or safety emergency exception that is the primary subject of these FAQs. Where a student is placed in a private school for the provision of Individualized Education Program (IEP) services on behalf of a school or school district subject to FERPA, the education records of the privately placed student that are maintained by the private school are subject both to FERPA and to the confidentiality requirements under Part B of the IDEA.

Questions and Answers on the Applicability of FERPA to Disclosures Related to COVID-19 ("Coronavirus")

1. Do parents and eligible students have to provide consent before an educational agency or institution discloses PII from education records?

Generally, yes. A parent or eligible student must provide written consent before an educational agency or institution discloses PII from a student's education records, unless one of the exceptions to FERPA's general consent rule applies. 20 U.S.C. §§ 1232g(b)(1) and (b)(2); 34 C.F.R. §§ 99.30 and 99.31. FERPA requires that a consent form be signed and dated by a parent or eligible student and (1) specify the records that may be disclosed; (2) state the purpose of the disclosure; and (3) identify the party or class of parties to whom the disclosure may be made. 34 C.F.R. § 99.30(a) and (b). At the conclusion of this document, we have included a sample FERPA consent form.

2. How does the health or safety emergency exception to FERPA's consent requirement permit an educational agency or institution to disclose PII from the education records of affected students?

Although educational agencies and institutions can often address threats to the health or safety of students or other individuals in a manner that does not identify a particular student, FERPA permits educational agencies and institutions to disclose, without prior written consent, PII from student education records to appropriate parties in connection with an emergency, if knowledge of that information is necessary to protect the health or safety of a student or other individuals. 20 U.S.C. § 1232g(b)(1)(I); 34 C.F.R. §§ 99.31(a)(10) and 99.36. This "health or safety emergency" exception to FERPA's general consent requirement is limited in time to the period of the emergency and generally does not allow for a blanket release of PII from student education records. Typically, law enforcement officials, public health officials, trained medical personnel, and parents (including parents of an eligible student) are the types of appropriate parties to whom PII from education records may be disclosed under this FERPA exception.

For purposes of FERPA's health or safety emergency exception, the determination by an educational agency or institution that there is a specific emergency is not based on a generalized or distant threat of a possible or eventual emergency for which the likelihood of occurrence is unknown, such as would be addressed in general emergency preparedness activities. If local public health authorities determine that a public health emergency, such as COVID-19, is a significant threat to students or other individuals in the community, an educational agency or institution in that community may determine that an emergency exists as well.

Under the FERPA health or safety emergency exception, an educational agency or institution is responsible for making a determination, on a case-by-case basis, whether to disclose PII from education records, and it may take into account the totality of the circumstances pertaining to the threat. *See* 34 C.F.R. § 99.36(c). If the educational agency or institution determines that there is an articulable and significant threat to the health or safety of the student or another individual and that certain parties need the PII from education records, to protect the health or safety of the

student or another individual, it may disclose that information to such parties without consent. This is a flexible standard under which the Department will not substitute its judgment for that of the educational agency or institution so that the educational agency or institution may bring appropriate resources to bear on the situation, provided that, based on the information available at the time of the educational agency's or institution's determination, there is a rational basis for such determination. We note also that, within a reasonable period of time after a disclosure is made under this exception, an educational agency or institution must record in the student's education records the articulable and significant threat that formed the basis for the disclosure and the parties to whom information was disclosed. 34 C.F.R. § 99.32(a)(5).

3. May student education records, such as health records, maintained by an educational agency or institution be disclosed, without consent, to public health departments if the educational agency or institution believes that the virus that causes COVID-19 poses a serious risk to the health or safety of an individual student in attendance at the educational agency or institution?

Yes. If an educational agency or institution, taking into account the totality of the circumstances, determines that an articulable and significant threat exists to the health or safety of a student in attendance at the agency or institution (or another individual at the agency or institution) as a result of the virus that causes COVID-19, it may disclose, without prior written consent, PII from student education records to appropriate officials at a public health department who need the information to protect the health or safety of the student (or another individual). Public health department officials may be considered "appropriate parties" by an educational agency or institution under FERPA's health or safety emergency exception, even in the absence of a formally declared health emergency. Typically, public health officials and trained medical personnel are among the types of appropriate parties to whom PII from education records, may be non-consensually disclosed under FERPA's health or safety emergency exception.

4. If an educational agency or institution learns that student(s) in attendance at the school are out sick due to COVID-19, may it disclose information about the student's illness under FERPA to other students and their parents in the school community without prior written parental or eligible student consent?

It depends, but generally yes, but only if that information is in a non-personally identifiable form. Specifically, the the educational agency or institution must make a reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information. *See* 34 C.F.R. § 99.31(b)(1). If an educational agency or institution discloses information about students in non-personally identifiable form, then consent by the parents or eligible students is not needed under FERPA. For example, if an educational agency or institution releases the fact that individuals are absent due to COVID-19 (but does not disclose their identities), this would generally not be considered personally identifiable to the absent students under FERPA as long as there are other individuals at the educational agency or institution who are absent for other reasons. However, we caution educational agencies or institutions to ensure that in releasing such facts, they do so in a manner that does not disclose other information that, alone or in combination, would allow a reasonable

person in the school community to identify the students who are absent due to COVID-19 with reasonable certainty.

5. May educational agencies and institutions disclose without consent the names, addresses, and phone numbers of absent students to the public health department so that the health department may contact their parents in order to assess the students' illnesses?

FERPA permits educational agencies and institutions to non-consensually disclose PII from education records in the form of contact information of absent students to the public health department in specific circumstances, such as in connection with a health or safety emergency (20 U.S.C. § 1232g(b)(1)(I); 34 C.F.R. §§ 99.31(a)(10) and 99.36) or pursuant to other applicable exceptions.

While FERPA generally permits the nonconsensual disclosure of properly designated "directory information" (e.g., name, address, phone number, grade level) when parents or eligible students have not opted out of such a disclosure, it does not permit an educational agency or institution to disclose "directory information" on students that is linked to non-directory information (such as information regarding a student's illness). For instance, an educational agency or institution may not disclose directory information on all students who are receiving special education services or those who have been absent from school.

Therefore, unless a specific FERPA exception applies, educational agencies and institutions should prepare consent forms for parents and eligible students to sign to allow the potential sharing of this type of information if they create, or intend to create, a tracking or monitoring system to identify an outbreak before an emergency is recognized.

6. If an educational agency or institution determines that a health or safety emergency exists, may it disclose, without consent, PII from student education records to the media?

No. As explained previously, FERPA only permits nonconsensual disclosures of PII from students' education records under the health or safety emergency exception to "appropriate parties" (such as public health officials) whose knowledge of the information is necessary to protect the health or safety of students or other individuals. While the media may have a role in alerting the community of an outbreak, they are not "appropriate parties" under FERPA's health or safety emergency exception because they generally do not have a role in protecting individual students or other individuals at the educational agency or institution. "Appropriate parties" in this context are normally parties who provide specific medical or safety attention, such as public health and law enforcement officials.

7. May the school identify a particular student, a teacher, or other school official as having COVID-19 to parents of other students in the school?

In most cases, it is sufficient to report the fact that an individual in the school has been determined to have COVID-19, rather than specifically identifying the student who is infected. School notification is an effective method of informing parents and eligible students of an illness

in the school. For settings in which parents are primarily doing drop-offs and pick-ups, posting signs on the doors may be effective. In other settings, sending home or e-mailing a notification may also be effective. These methods serve to notify parents and eligible students of a potential risk, which may be particularly important for students who may be more susceptible to infection or to developing severe complications from an infection, and to alert parents to look for symptoms in their own children and eligible students to more closely monitor themselves for symptoms.

Nothing in FERPA prevents schools from telling parents and students that a specific teacher or other school official has COVID-19 because FERPA applies to students' education records, not records on school officials. However, there may be State laws that apply in these situations.

There may be a rare situation during a health or safety emergency, however, in which schools may determine (in conjunction with health, law enforcement, or other such officials) that parents of students or eligible students are appropriate parties to whom to disclose identifiable information about a student with COVID-19. For example, school officials may determine that it is appropriate to disclose identifiable information about of a student with COVID-19 to parents of other students if parents need to know this information to take appropriate action to protect the health or safety of their children. For example if a student with COVID-19 is a wrestler and has been in direct and close contact with other students who are on the team or who are in the school and have higher health risks, school officials may determine it necessary to disclose the identity of the diagnosed student to the parents of the other students. In these limited situations, parents and eligible students may need to be aware of this information in order to take appropriate precautions or other actions to ensure the health or safety of their child or themselves, especially if their child or they may have a higher risk of susceptibility to COVID-19 or of developing severe complications from COVID-19.[4] School officials should make the determination on a case-by-case basis whether a disclosure of the student's name is absolutely necessary to protect the health or safety of students or other individuals or whether a general notice is sufficient, taking into account the totality of the circumstances, including the needs of such students or other individuals to have such information in order to take appropriate protective action(s) and the risks presented to the health or safety of such students or other individuals.

8. May an educational agency or institution disclose PII from an eligible student's education records to the student's parents if the eligible student has been determined to have COVID-19?

Yes, for dependent students and generally yes, but see below. Under FERPA, an educational agency or institution, including an institution of postsecondary education, may disclose, without the eligible student's written consent, PII from an eligible student's education records to his or her parents under certain conditions. For example, a university physician treating an eligible student for COVID-19 might determine that the student's treatment records should be disclosed to the student's parents. This disclosure may be made, without consent of the eligible student, if the parents claim the eligible student as a dependent under section 152 of the Internal Revenue Code of

[4] For helpful information on risk, please see the Centers for Disease Control and Prevention's current risk assessment, which is available at: https://www.cdc.gov/coronavirus/2019-ncov/specific-groups/children-faq.html.

1986. 20 U.S.C. § 1232g(b)(1)(H); 34 C.F.R. § 99.31(a)(8). If the parents do not claim the eligible student as a dependent, then the disclosure may be made to the parents, without the eligible student's written consent, if the disclosure is in connection with a health or safety emergency provided certain conditions are satisfied (as discussed in the response to question two above). 20 U.S.C. § 1232g(b)(1)(I); 34 C.F.R. §§ 99.31(a)(10) and 36.

9. What if a parent of a student who is not an eligible student refuses to provide written consent to permit the release of PII contained in student education records to the public health department?

FERPA permits educational agencies and institutions to release information from education records without consent after the removal of all PII, provided that the agency or institution has made a reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information. 34 C.F.R. § 99.31(b)(1). Thus, it would be problematic to disclose that every student in a particular class or grade level is absent if there is, for instance, a directory with the names of every student in that class or grade. Therefore, it is prudent that educational agencies or institutions obtain written consent to permit the disclosure of PII from students' education records to the public health department. If the parent or eligible student will not provide written consent for the disclosure of the PII, then the educational agency or institution may not make the disclosure unless it has determined that there is an applicable exception to the general requirement of consent that permits the disclosure, such as if a health or safety emergency exists and the PII is disclosed to an appropriate party whose knowledge of the information is necessary to protect the health or safety of the student or other individuals.

10. Is an educational agency or institution required to record disclosures of PII from student education records submitted to the public health department or other outside parties, even in connection with a health or safety emergency?

Yes. FERPA generally requires educational agencies and institutions to maintain a record of each request for access to and each disclosure of PII from the education records of each student. 34 C.F.R. § 99.32(a)(1). Moreover, when making a disclosure under the health or safety emergency provision in FERPA, educational agencies and institutions are specifically required to record the articulable and significant threat to the health or safety of a student or other individual that formed the basis for the disclosure and the parties to whom the agency or institution disclosed the information. 34 C.F.R. § 99.32(a)(5). The record of each request for access to and each disclosure of PII from student education records must be maintained with the education records of each student as long as the records are maintained. 34 C.F.R. § 99.32(a)(2). This requirement enables parents and eligible students who do not provide written consent for disclosure of education records to see the circumstances under which and the parties to whom their information was disclosed. However, educational agencies and institutions are not required to record disclosures for which the parent or eligible student has provided written consent. 34 C.F.R. § 99.32(d)(3).

****

The Department's Student Privacy Policy Office or SPPO is the office that administers FERPA. SPPO is available to respond to questions school officials may have about FERPA. School officials may e-mail questions to SPPO at FERPA@ed.gov. You may also call us at (202) 260-3887. Additional information and guidance on FERPA is available on SPPO's website at: https://studentprivacy.ed.gov/.

The Department has a list of resources regarding COVID-19 (coronavirus) on our website at https://www.ed.gov/coronavirus. Questions related to the coronavirus may be emailed to the Department at COVID-19@ed.gov.

In December 2019, the U.S. Department of Education, along with HHS, issued guidance on the applicability of FERPA and the HIPAA to student health records, the "Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) To Student Health Records." *See* https://studentprivacy.ed.gov/sites/default/files/resource_document/file/2019%20HIPAA%20FERPA%20Joint%20Guidance%20508.pdf. This 2019 document updated the Department's 2008 guidance and explained that the HIPAA Privacy Rule does not apply to education records that are protected by FERPA. Student health records that are maintained by a public elementary and secondary educational agency or institution or by a party acting for the agency or institution are "education records" subject to FERPA, and school officials must follow the requirements of FERPA in making any disclosures of the PII from these records. At the postsecondary level, FERPA applies to most public and private institutions of postsecondary education and to the student health records that they maintain. Such student health records may either constitute "education records" or "treatment records," if certain conditions are met, but in either case they are subject to FERPA and not the HIPAA Privacy Rule.

For more information on the HIPAA Privacy Rule, please visit HHS' HIPAA Privacy Rule website at: http://www.hhs.gov/ocr/privacy/. The website offers a wide range of helpful information about the HIPAA Privacy Rule, including frequently asked questions.

[Sample FERPA Consent Form]

Disclosure of Information Protected by the Family Educational Rights and Privacy Act by _____ [Name of School/School District] to [Name of Appropriate Authority]

Pursuant to the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 C.F.R. part 99), the written consent of a parent or eligible student is required before the education records of a student, or personally identifiable information contained therein, may be disclosed to a third party, unless an exception to this general requirement of written consent applies. If a student is age 18 years or older, or is enrolled in an institution of postsecondary education, he or she is an "eligible student" and must provide written consent for the disclosure of his or her education records or personally identifiable information contained therein.

I,_____, hereby agree to allow _____
[SCHOOL OR DISTRICT NAME] to disclose the following personally identifiable information or education records:
_____ [Specify education records or personally identifiable information that may be disclosed] on _____
[Name of Student] to _____[Name of Appropriate Authority] for the purpose of [State purpose of disclosure] _____.

You may withdraw your consent to share this information at any time. A request to withdraw your consent should be submitted in writing and signed.

_____
Signature of Parent, Guardian, or Eligible Student

Date:_____

STUDENT PRIVACY POLICY OFFICE
FERPA and Virtual Learning Related Resources
March 2020

As educators and students move to virtual learning during this time of social distancing due to COVID-19, the Student Privacy Policy Office (SPPO) has received questions about available resources on virtual learning and the Family Educational Rights and Privacy Act (FERPA).

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 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. (An "eligible student" is a student who has turned 18 or is attending college at any age.) 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. 20 U.S.C. 1232g; 34 C.F.R. Part 99.

Two key resources on our website are:

- *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* — this resource identifies applicable exceptions under FERPA, including the school official exception. This resource, while originally developed for online educational services, is also applicable for virtual learning tools and includes best practices for safeguarding student education records under FERPA.

- *Protecting Student Privacy While Using Online Educational Services: Model Terms of Service* — this checklist is a helpful tool to evaluate online educational apps.

These two resources are part of our Security Best Practices, which includes additional resources on safeguarding education records.

There are also additional resources on related topics under FERPA, including classroom observations, use of emails, videos, and other virtual learning tools. 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.

- Our Letter to Mamas on classroom observation is also applicable to virtual classrooms.
- Our video, Email and Student Privacy, identifies best practices for emails.
- With regard to videos and virtual classrooms, to the extent videos are recorded and maintained as education records, the FAQs on Photos and Videos under FERPA might be useful.

Additionally, the recently-released FERPA and the Coronavirus Disease 2019 (COVID-19) FAQs document identifies questions for school officials regarding the health or safety emergency exception under FERPA in the context of COVID-19.

SPPO is available to assist you with your student privacy questions under FERPA. Additional information is on our website at https://studentprivacy.ed.gov.

Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices

Overview

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems. More PTAC information is available on https://studentprivacy.ed.gov.

PTAC welcomes input on this document and suggestions for future technical assistance resources relating to student privacy. Comments and suggestions can be sent to PrivacyTA@ed.gov.

Purpose

Recent advances in technology and telecommunications have dramatically changed the landscape of education in the United States. Gone are the days when textbooks, photocopies, and filmstrips supplied the entirety of educational content to a classroom full of students. Today's classrooms increasingly employ on-demand delivery of personalized content, virtual forums for interacting with other students and teachers, and a wealth of other interactive technologies that help foster and enhance the learning process. Online forums help teachers share lesson plans; social media help students collaborate across classrooms; and web-based applications assist teachers in customizing the learning experience for each student to achieve greater learning outcomes.

Early adopters of these technologies have demonstrated their potential to transform the educational process, but they have also called attention to possible challenges. In particular, the information sharing, web-hosting, and telecommunication innovations that have enabled these new education technologies raise questions about how best to protect student privacy during use. This document will address a number of these questions, and present some requirements and best practices to consider, when evaluating the use of online educational services.

What are Online Educational Services?

This document will address privacy and security considerations relating to computer software, mobile applications (apps), and web-based tools provided by a third-party to a school or district that students and/or their parents access via the Internet and use as part of a school activity. Examples include online services that students use to access class readings, to view their learning progression, to watch

video demonstrations, to comment on class activities, or to complete their homework. This document does not address online services or social media that students may use in their personal capacity outside of school, nor does it apply to online services that a school or district may use to which students and/or their parents do not have access (e.g., an online student information system used exclusively by teachers and staff for administrative purposes).

Many different terms are used to describe both the online services discussed in this document (e.g., Ed Tech, educational web services, information and communications technology, etc.) and the companies and other organizations providing these services. This document will use the term "online educational services" to describe this broad category of tools and applications, and the term "provider" to describe the third-party vendors, contractors, and other service providers that make these services available to schools and districts.

Is Student Information Used in Online Educational Services Protected by FERPA?

It depends. Because of the diversity and variety of online educational services, there is no universal answer to this question. The Family Educational Rights and Privacy Act (FERPA) (see 20 U.S.C. § 1232g and 34 CFR Part 99) protects personally identifiable information (PII) from students' education records from unauthorized disclosure. FERPA defines education records as "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" (see 34 CFR § 99.3 definition of "education record"). FERPA also defines the term PII, which includes direct identifiers (such as a student's or other family member's name) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name) (see 34 CFR § 99.3 definition of "personally identifiable information"). For more information about FERPA, please visit the Family Policy Compliance Office's Web site at https://studentprivacy.ed.gov.

Some types of online educational services do use FERPA-protected information. For example, a district may decide to use an online system to allow students (and their parents) to log in and access class materials. In order to create student accounts, the district or school will likely need to give the provider the students' names and contact information from the students' education records, which are protected by FERPA. Conversely, other types of online educational services may not implicate FERPA-protected information. For example, a teacher may have students watch video tutorials or complete interactive exercises offered by a provider that does not require individual students to log in. In these cases, no PII from the students' education records would be disclosed to (or maintained by) the provider.

Online educational services increasingly collect a large amount of contextual or transactional data as part of their operations, often referred to as "metadata." Metadata refer to information that provides meaning and context to other data being collected; for example, information about how long a particular student took to perform an online task has more meaning if the user knows the date and time when the student completed the activity, how many attempts the student made, and how long the student's mouse hovered over an item (potentially indicating indecision).

Metadata that have been stripped of all direct and indirect identifiers are not considered protected information under FERPA because they are not PII. A provider that has been granted access to PII from education records under the school official exception may use any metadata that are not linked to FERPA-protected information for other purposes, unless otherwise prohibited by the terms of their agreement with the school or district.

Schools and districts will typically need to evaluate the use of online educational services on a case-by-case basis to determine if FERPA-protected information (i.e., PII from education records) is implicated. If so, schools and districts must ensure that FERPA requirements are met (as well as the requirements of any other applicable federal, state, tribal, or local laws).

EXAMPLE 1: A district enters into an agreement to use an online tutoring and teaching program and discloses PII from education records needed to establish accounts for individual students using FERPA's school official exception. The provider sends reports on student progress to teachers on a weekly basis, summarizing how each student is progressing. The provider collects metadata about student activity, including time spent online, desktop vs. mobile access, success rates, and keystroke information. If the provider de-identifies these metadata by removing all direct and indirect identifying information about the individual students (including school and most geographic information), the provider can then use this information to develop new personalized learning products and services (unless the district's agreement with the provider precludes this use).

What Does FERPA Require if PII from Students' Education Records is Disclosed to a Provider?

It depends. Because of the diversity and variety of online educational services, there is no universal answer to this question. Subject to exceptions, the general rule under FERPA is that a school or district cannot disclose PII from education records to a provider unless the school or district has first obtained written consent from the parents (or from "eligible students," i.e., those who are 18 years of age or older or attending a postsecondary school). Accordingly, schools and districts must either obtain consent, or ensure that the arrangement with the provider meets one of FERPA's exceptions to the written consent requirement.

While disclosures of PII to create user accounts or to set up individual student profiles may be accomplished under the "directory information" exception, more frequently this type of disclosure will be made under FERPA's school official exception. "Directory information" is information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed (see 34 CFR § 99.3 definition of "directory information"). Typical examples of directory information include student name and address. To disclose student information under this exception, individual school districts must establish the specific elements or categories of directory information that they intend to disclose and publish those elements or categories in a public notice. While the directory information exception can seem to be an easy way to share PII from education

records with providers, this approach may be insufficient for several reasons. First, only information specifically identified as directory information in the school's or district's public notice may be disclosed under this exception. Furthermore, parents (and eligible students) generally have the right to "opt out" of disclosures under this exception, thereby precluding the sharing of information about those students with providers. Given the number of parents (and eligible students) who elect to opt out of directory information, schools and districts may not find this exception feasible for disclosing PII from education records to providers to create student accounts or profiles.

The FERPA school official exception is more likely to apply to schools' and districts' use of online educational services. Under the school official exception, schools and districts may disclose PII from students' education records to a provider as long as the provider:

1. Performs an institutional service or function for which the school or district would otherwise use its own employees;

2. Has been determined to meet the criteria set forth in in the school's or district'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 school or district with regard to 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 school or district to do so and it is otherwise permitted by FERPA).

See 34 CFR § 99.31(a)(1)(i).

Two of these requirements are of particular importance. First, the provider of the service receiving the PII must have been determined to meet the criteria for being a school official with a "legitimate educational interest" as set forth in the school's or district's annual FERPA notification. Second, the framework under which the school or district uses the service must satisfy the "direct control" requirement by restricting the provider from using the PII for unauthorized purposes. While FERPA regulations do not require a written agreement for use in disclosures under the school official exception, in practice, schools and districts wishing to outsource services will usually be able to establish direct control through a contract signed by both the school or district and the provider. In some cases, the "Terms of Service" (TOS) agreed to by the school or district, prior to using the online educational services, may contain all of the necessary legal provisions governing access, use, and protection of the data, and thus may be sufficient to legally bind the provider to terms that are consistent with these direct control requirements.

When disclosing PII from education records to providers under the school official exception, schools and districts should be mindful of FERPA's provisions governing parents' (and eligible students') access to the students' education records. Whenever a provider maintains a student's education records, the

school and district must be able to provide the requesting parent (or eligible student) with access to those records. Schools and districts should ensure that their agreements with providers include provisions to allow for direct or indirect parental access. Under FERPA, a school must comply with a request from a parent or eligible student for access to education records within a reasonable period of time, but not more than 45 days after it has received the request. Some States have laws that require access to education records sooner than 45 days.

Schools and districts are encouraged to remember that FERPA represents a minimum set of requirements to follow. Thus, even when sharing PII from education records under an exception to FERPA's consent requirement, it is considered a best practice to adopt a comprehensive approach to protecting student privacy when using online educational services.

Do FERPA and the Protection of Pupil Rights Amendment (PPRA) Limit What Providers Can Do with the Student Information They Collect or Receive?

On occasion, providers may seek to use the student information they receive or collect through online educational services for other purposes than that for which they received the information, like marketing new products or services to the student, targeting individual students with directed advertisements, or selling the information to a third party. If the school or district has shared information under FERPA's school official exception, however, the provider cannot use the FERPA-protected information for any other purpose than the purpose for which it was disclosed.

Any PII from students' education records that the provider receives under FERPA's school official exception may only be used for the specific purpose for which it was disclosed (i.e., to perform the outsourced institutional service or function, and the school or district must have direct control over the use and maintenance of the PII by the provider receiving the PII). Further, under FERPA's school official exception, the provider may not share (or sell) FERPA-protected information, or re-use it for any other purposes, except as directed by the school or district and as permitted by FERPA.

It is important to remember, however, that student information that has been properly de-identified or that is shared under the "directory information" exception, is not protected by FERPA, and thus is not subject to FERPA's use and re-disclosure limitations.

EXAMPLE 2: A district contracts with a provider to manage its cafeteria account services. Using the school official exception, the district gives the provider student names and other information from school records (not just directory information). The provider sets up an online system that allows the school, parents, and students to access cafeteria information to verify account balances and review the students' meal selections. The provider cannot sell the student roster to a third party, nor can it use PII from education records to target students for advertisements for foods that they often purchase at school under FERPA because the provider would then be using FERPA-protected information for different purposes than those for which the information was shared.

FERPA is not the only statute that limits what providers can do with student information. The Protection of Pupil Rights Amendment (PPRA) provides parents with certain rights with regard to some marketing activities in schools. Specifically, PPRA requires that a school district must, with exceptions, directly notify parents of students who are scheduled to participate in activities involving the collection, disclosure, or use of personal information collected from students for marketing purposes, or to sell or otherwise provide that information to others for marketing purposes, and to give parents the opportunity to opt-out of these activities. 20 U.S.C. § 1232h(c)(2)(C)(i). Subject to the same exceptions, PPRA also requires districts to develop and adopt policies, in consultation with parents, about these activities. 20 U.S.C. § 1232h(c)(1)(E) and (c)(4)(A). PPRA has an important exception, however, as neither parental notice and the opportunity to opt-out nor the development and adoption of policies are required for school districts to use students' personal information that they collect from students for the exclusive purpose of developing, evaluating, or providing educational products or services for students or schools. 20 U.S.C. § 1232h(c)(4)(A).

While FERPA protects PII from education records maintained by a school or district, PPRA is invoked when personal information is collected from the student. The use of online educational services may give rise to situations where the school or district provides FERPA-protected data to open accounts for students, and subsequent information gathered through the student's interaction with the online educational service may implicate PPRA. Student information collected or maintained as part of an online educational service may be protected under FERPA, under PPRA, under both statutes, or not protected by either. Which statute applies depends on the content of the information, how it is collected or disclosed, and the purposes for which it is used.

It is important to remember that even though PPRA only applies to K-12 institutions, there is no time-limit on the limitations governing the use of personal information collected from students for marketing purposes. So, for example, while PPRA would not limit the use of information collected from college students for marketing, it would restrict the use of information collected from students while they were still in high school (if no notice or opportunity to opt-out was provided) even after those students graduate.

EXAMPLE 3: A district contracts with an online tutoring service using the school official exception. As part of the service, the provider uses data about individual students to personalize learning modules for the district's students. This does not implicate the PPRA because the activity falls under the PPRA exception for educational services and products. This use of data about individual students is similarly permissible under FERPA because the provider is only using any FERPA-protected information for the purposes for which it was shared.

EXAMPLE 4: A district contracts under the school official exception with a provider for basic productivity applications to help educate students: email, calendaring, web-search, and document collaboration software. The district sets up the user accounts, using basic enrollment information (name, grade, etc.) from student records. Under FERPA, the provider may not use data about individual student preferences gleaned from scanning student content to target ads to individual students for clothing or toys, because using the data for these purposes was not authorized by the district and does not constitute a legitimate educational interest as specified in the district's annual notification of FERPA rights.

PPRA would similarly prohibit targeted ads for clothing or toys, unless the district had a policy addressing this and parents were notified and given the opportunity to opt-out of such marketing. In spite of these limitations, however, the provider may use data (even in individually identifiable form) to improve its delivery of these applications, including spam filtering and usage monitoring. The provider may also use any non-PII data, such as metadata with all direct and indirect identifiers removed, to create new products and services that the provider could market to schools and districts.

Schools and districts should be aware that neither FERPA nor the PPRA absolutely prohibits them from allowing providers to serve generalized, non-targeted advertisements. FERPA would not prohibit, for example, a school from selling space on billboards on the football field, nor would it prohibit a school or district from allowing a provider acting as a school official from serving ads to all students in email or other online services.

Finally, schools and districts should remember their important role in setting policies to protect student privacy. While FERPA and PPRA provide important protections for student information, additional use or disclosure restrictions may be advisable depending on the situation and the sensitivity of the information. Any additional protections that a school or district would like to require should be documented in the written agreement (the contract or TOS) with the provider.

What are Some Other Best Practices for Protecting Student Privacy When Using Online Educational Services?

Regardless of whether FERPA or PPRA applies to a school's or district's proposed use of online educational services, the Department recommends that schools and districts follow privacy, security, and transparency best practices, such as:

- **Maintain awareness of other relevant federal, state, tribal, or local laws.**

  FERPA and PPRA are not the only laws that protect student information. Other federal, state, tribal, or local laws may apply to online educational services, and may limit the information that can be shared with providers. In particular, schools and districts should be aware of and

consider the requirements of the Children's Online Privacy and Protection Act (COPPA) before using online educational services for children under age 13. In general, COPPA applies to commercial Web sites and online services directed to children and those Web sites and services with actual knowledge that they have collected personal information from children. Absent an exception, these sites must obtain verifiable parental consent prior to collecting personal information from children. The Federal Trade Commission (FTC) has interpreted COPPA to allow schools to exercise consent on behalf of parents in certain, limited circumstances (see http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#Schools).

- **Be aware of which online educational services are currently being used in your district.**

  Conduct an inventory of the online educational services currently being used within your school or district. Not only will this help assess the scope and range of student information being shared with providers, but having a master list of online educational services will help school officials to collaboratively evaluate which services are most effective, and help foster informed communication with parents.

- **Have policies and procedures to evaluate and approve proposed online educational services**.

  Establish and enforce school and district-wide policies for evaluating and approving online educational services prior to implementation. Schools and districts should be clear with both teachers and administrators about how proposed online educational services can be approved, and who has the authority to enter into agreements with providers. This is true not only for formal contracts, but also for consumer-oriented "Click-Wrap" software that is acquired simply by clicking "accept" to the provider's TOS. With Click-Wrap agreements, the act of clicking a button to accept the TOS serves to enter the provider and the end-user (in this case, the school or district) into a contractual relationship akin to signing a contract.

  Most schools or districts already have processes in place for evaluating vendor contracts for privacy and security considerations; using these established procedures may be the most effective way to evaluate proposed online educational services. It is particularly important that teachers and staff not bypass internal controls in the acquisition process when deciding to use free online educational services. To ensure that privacy and security concerns relating to these free services are adequately considered, the Department recommends that free online educational services go through the same (or a similar) approval process as paid educational services to ensure that they do not present a risk to the privacy or security of students' data or to the schools and district's IT systems. Following standard internal controls, including testing, will also enable the schools and district's IT personnel to assist in the implementation process. Simple and more streamlined processes will, of course, generate greater compliance.

- **When possible, use a written contract or legal agreement.**

  As mentioned above, the use of online educational services usually involves some form of a

contract or legal agreement between the school and the provider. Having a written contract or legal agreement helps schools and districts maintain the required "direct control" over the use and maintenance of student data. Even when FERPA is not implicated, the Department recommends using written agreements as a best practice. When drafting and reviewing these contracts, the Department recommends the inclusion of certain provisions:

- Security and Data Stewardship Provisions. Make clear whether the data collected belongs to the school/district or the provider, describe each party's responsibilities in the event of a data breach (see PTAC's Data Breach Response Checklist), and, when appropriate, establish minimum security controls that must be met and allow for a security audit.

- Collection Provisions. Be specific about the information the provider will collect (e.g., forms, logs, cookies, tracking pixels, etc.).

- Data Use, Retention, Disclosure, and Destruction Provisions. Define the specific purposes for which the provider may use student information, and bind the provider to only those approved uses. If student information is being shared under the school official exception to consent in FERPA, then it would also be a best practice to specify in the agreement how the school or district will be exercising "direct control" over the third party provider's use and maintenance of the data. Specify with whom the provider may share (re-disclose) student information, and if PII from students' education records is involved, ensure that these provisions are consistent with FERPA. Include data archival and destruction requirements to ensure student information is no longer residing on the provider's systems after the contract period is complete. When appropriate, define what disclosure avoidance procedures must be performed to de-identify student information before the provider may retain it, share it with other parties, or use it for other purposes.

- Data Access Provisions. Specify whether the school, district and/or parents (or eligible students) will be permitted to access the data (and if so, to which data) and explain the process for obtaining access. This is especially important if the online educational services will be creating new education records that will be maintained by the provider on behalf of the school or district, as FERPA's requirements regarding parental (or eligible students') access will then apply. To avoid the challenges involved in proper authentication of students' parents by the provider, the Department recommends that the school or district serve as the intermediary for these requests, wherein the parent requests access to any education records created and maintained by the provider directly from the school or district, and the school or district then obtains the records from the provider to give back to the parent.

- Modification, Duration, and Termination Provisions. Establish how long the agreement will be in force, what the procedures will be for modifying the terms of the agreement

(mutual consent to any changes is a best practice), and what both parties' responsibilities will be upon termination of the agreement, particularly regarding disposition of student information maintained by the provider.

- Indemnification and Warranty Provisions. Carefully assess the need for and legality of any such provisions and determine whether applicable state or tribal law prohibits or limits the school's or district's ability to indemnify a provider. Analyze whether there should be indemnification provisions in which the provider agrees to indemnify the school or district, particularly relating to a school's or district's potential liabilities resulting from a provider's failure to comply with applicable federal, state, or tribal laws. Given that the Department looks to schools and districts to comply with FERPA and PPRA, be specific about what you will require the provider to do in order to comply with applicable state and federal laws, such as FERPA and PPRA, and what the provider agrees to do to remedy a violation of these requirements and compensate the school or district for damages resulting from the provider's violation.

- **Extra steps are necessary when accepting Click-Wrap licenses for consumer apps.**

  Schools and districts sometimes can't negotiate agreements with providers of consumer apps, and are faced with a choice to accept the providers' TOS or not use the app. Extra caution and extra steps are warranted before employing Click-Wrap consumer apps:

  - Check Amendment Provisions. In addition to reviewing for the above terms, you should review the TOS to determine if the provider has retained the right to amend the TOS without notice. If the provider will be using FERPA-protected information, schools and districts should exercise caution when entering into Click-Wrap agreements that allow for amendment without notice, given FERPA's requirement to maintain "direct control" over the use and maintenance of the information under the school official exception. It is a best practice to review these agreements regularly to determine if any provisions have changed, and if so, to re-evaluate whether to continue using the service.

  - Print or Save the TOS. When accepting a Click-Wrap agreement, you should save a copy of the TOS that you have agreed to. You can either download and save a digital copy, or print and file a copy.

  - Limit Authority to Accept TOS. One potential issue with Click-Wrap agreements is that they can be easily accepted, without going through normal district or school approval channels. Individual teachers may not understand the specifics of how the provider will use and secure student data. Districts or schools should develop policies outlining when individual teachers may download and use Click-Wrap software.

EXAMPLE 5: A teacher who has many remote students wants to foster increased collaboration and socialization among her students. Pursuant to her district's policy, she selects a service from a district-approved list of providers, and accepts the provider's Click-Wrap agreement before creating the user accounts for all students (including those who opted out of directory information). Her students successfully participate in a students-only social collaboration space.

EXAMPLE 6: A teacher wants students to be able to share photographs and videos online and identifies an app that will allow this sharing. He creates user accounts for all students (including those who opted out of directory information) and accepts the app's Click-Wrap agreement without reading it. The TOS allow the provider to use the information for a variety of non-educational purposes, including selling merchandise. The district discovers that this service is being used and determines that the TOS violate FERPA. The district proceeds to block access to the service from district computers, and begins negotiations with the provider to delete the user accounts and any information attached to them.

- **Be transparent with parents and students.**

  The Department encourages schools and districts to be as transparent as possible with parents and students about how the school or district collects, shares, protects, and uses student data. FERPA requires that schools and districts issue an annual notification to parents and eligible students explaining their rights under FERPA (34 CFR § 99.7), and many schools and districts elect to combine their directory information policy public notice, required pursuant to §99.37 of the regulations, with their annual notice of rights. PPRA also requires schools and districts to provide parents and students with effective notice of their PPRA rights, to provide notice to parents of district policies (developed and adopted in consultation with parents) regarding specific activities, and to notify them of the dates of specific events and the opportunity to opt out of participating in those events. Beyond FERPA and PPRA compliance, however, the Department recommends that schools and districts clearly explain on their Web sites how and with whom they share student data, and that they post any school and district policies on outsourcing of school functions, including online educational services. Schools and districts may also want to post copies of the privacy and security provisions of important third party contracts.

  With online educational services, it can often be unclear what information is being collected while students are using the technology. Even when this information is not protected by FERPA or other privacy laws, it is a best practice to inform students and their parents of what information is being collected and how it will be used. When appropriate, the Department recommends that schools or districts develop an education technology plan that addresses student privacy and information security issues, and solicit feedback from parents about the plan prior to its implementation or the adoption of new online education services.

Transparency provides parents, students, and the general public with important information about how the school or district protects the privacy of student data. Greater transparency enables parents, students, and the public to develop informed opinions about the benefits and risks of using education technology and helps alleviate confusion and misunderstandings about what data will be shared and how they will be used.

- **Consider that parental consent may be appropriate.**

  Even in instances where FERPA does not require parental consent, schools and districts should consider whether consent is appropriate. These are individual determinations that should be made on a case-by-case basis.

Additional Resources

Materials below include links to resources that provide additional best practice recommendations and guidance relating to use of online educational services. Please note that these resources do not necessarily address the particular legal requirements, including FERPA, that your school and district need to meet when collecting, storing, disseminating, or releasing education records to a provider. It is always a best practice to consult legal counsel to determine the applicable federal, state, tribal, and local requirements prior to entering into contractual agreements with providers. Some resources prepared by third-party experts are included as well.

- Family Policy Compliance Office, U.S. Department of Education, *Model Notice for Directory Information:* https://studentprivacy.ed.gov/resources/model-notice-directory-information
- National Institute of Standards and Technology, Computer Security Resource Center: http://csrc.nist.gov/publications/
- National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing* (2011): http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
- National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publications (FIPS) 199* (2004): http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- Privacy Technical Assistance Center, U.S. Department of Education: https://studentpriavcy.ed.gov
- Privacy Technical Assistance Center, U.S. Department of Education, *Checklist – Data Breach Response* (2012): https://studentprivacy.ed.gov/resources/data-breach-response-checklist
- Privacy Technical Assistance Center, U.S. Department of Education, *Written Agreement Checklist* (2012): https://studentpriavcy.ed.gov/resources/written-agreement-checklist
- U.S. Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions - COPPA AND SCHOOLS* (2013): http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#Schools
- U.S. Federal Trade Commission, *FTC Strengthens Kid's Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Protection Rule* (2012): http://www.ftc.gov/opa/2012/12/coppa.shtm

Glossary

Directory Information is 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, date and place of birth, participation in officially recognized activities and sports, and dates of attendance. 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." 34 CFR § 99.3 and 34 CFR § 99.37.

Education records means records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations. 34 CFR § 99.3.

Eligible Student means a student to whom FERPA rights have transferred upon turning 18 years of age, or upon enrolling in a post-secondary institution at any age. 34 CFR § 99.3.

Personally identifiable information (PII) is a FERPA term referring to identifiable information that is maintained in education records and includes direct identifiers, such as a student's name or identification number, indirect identifiers, such as a student's date of birth, or other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR § 99.3, for a complete definition of PII specific to education records and for examples of other data elements that are defined to constitute PII.

Personal Information Collected from Students is a PPRA term referring to individually identifiable information including a student or parent's first and last name; a home or other physical address (including street name and the name of the city or town); a telephone number; or a Social Security identification number collected from any elementary or secondary school student. 20 U.S.C. § 1232h(c)(6)(E).

School Official means any employee, including teacher, that the school or district has determined to have a "legitimate educational interest" in the personally identifiable information from an education record of a student. School officials may also include third party contractors, consultants, volunteers, service providers, or other party with whom the school or district has outsourced institutional services or functions for which the school or district would otherwise use employees under the school official exception in FERPA. 34 CFR § 99.31(a)(1).

FAQs on Photos and Videos under FERPA

1. When is a photo or video of a student an education record under FERPA?

As with any other "education record," a photo or video of a student is an education record, subject to specific exclusions, when the photo or video is: (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. (20 U.S.C. 1232g(a)(4)(A); 34 CFR § 99.3 "Education Record")[1]

Directly Related to a Student:

FERPA regulations do not define what it means for a record to be "directly related" to a student. In the context of photos and videos, determining if a visual representation of a student is *directly* related to a student (rather than just incidentally related to him or her) is often context-specific, and educational agencies and institutions should examine certain types of photos and videos on a case by case basis to determine if they directly relate to any of the students depicted therein. Among the factors that may help determine if a photo or video should be considered "directly related" to a student are the following:

- The educational agency or institution uses the photo or video for disciplinary action (or other official purposes) involving the student (including the victim of any such disciplinary incident);
- The photo or video contains a depiction of an activity:
    - that resulted in an educational agency or institution's use of the photo or video for disciplinary action (or other official purposes) involving a student (or, if disciplinary action is pending or has not yet been taken, that would reasonably result in use of the photo or video for disciplinary action involving a student);
    - that shows a student in violation of local, state, or federal law;
    - that shows a student getting injured, attacked, victimized, ill, or having a health emergency;
- The person or entity taking the photo or video intends to make a specific student the focus of the photo or video (e.g., ID photos, or a recording of a student presentation); or
- The audio or visual content of the photo or video otherwise contains personally identifiable information contained in a student's education record.

A photo or video should not be considered directly related to a student in the absence of these factors and if the student's image is incidental or captured only as part of the background, or if a student is shown participating in school activities that are open to the public and without a specific focus on any individual.

Examples of situations that may cause a video to be an education record:

- A school surveillance video showing two students fighting in a hallway, used as part of a disciplinary action, is directly related to the students fighting.
- A classroom video that shows a student having a seizure is directly related to that student because the depicted health emergency becomes the focus of the video.
- If a school maintains a close-up photo of two or three students playing basketball with a general view of student spectators in the background, the photo is directly related to the basketball players because they are the focus of the photo, but it is not directly related to the students pictured in the background. Schools often designate photos or videos of students participating in public events (e.g., sporting events, concerts, theater performances, etc.) as directory information and/or obtain consent from the parents or eligible students to publicly disclose photos or videos from these events.
- A video recording of a faculty meeting during which a specific student's grades are being discussed is directly related to that student because the discussion contains PII from the student's education record.

Maintained by an educational agency or institution:

To be considered an education record under FERPA, an educational agency or institution, or a party acting for the agency or institution, also must maintain the record. Thus, a photo taken by a parent at a school football game would not be considered an education record, even if it is directly related to a particular student, because it is not being maintained by the school or on the school's behalf. If, however, the parent's photo shows two students fighting at the game, and the parent provides a copy of the photo to the school, which then maintains the photo in the students' disciplinary records, then the copy of the photo being maintained by the school is an education record.

Exclusion for Law Enforcement Unit Records

The FERPA statute and regulations (20 U.S.C. 1232g(a)(4)(B)(ii) and 34 CFR §§ 99.3 and 99.8) exclude from the definition of education records those records created and maintained by a law enforcement unit of an educational agency or institution for a law enforcement purpose. Thus, if a law enforcement unit of an educational agency or institution creates and maintains the school's surveillance videos for a law enforcement purpose, then any such videos would not be considered to be education records. If the law enforcement unit provides a copy of the video to another component within the educational agency or institution (for example, to maintain the record in connection with a disciplinary action), then the copy of the video may become an education record of the student(s) involved if the video is not subject to any other exclusion from the definition of "education records" and the video is: (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.

2. Can the same recorded image be the education record of more than one student under FERPA?

Yes. For example, a surveillance video that shows two students fighting on a school bus that the school uses and maintains to discipline the two students, would be "directly related to" and, therefore, the education record of both students.

3. If a video is an education record for multiple students, can a parent of one of the students or the eligible student view the video?

When a video is an education record of multiple students, in general, FERPA requires the educational agency or institution to allow, upon request, an individual parent of a student (or the student if the student is an eligible student) to whom the video directly relates to inspect and review, or "be informed of" the content of the video, consistent with the FERPA statutory provisions in 20 U.S.C. § 1232g(a)(1)(A) and regulatory provisions at 34 CFR § 99.12(a). FERPA generally does not require the educational agency or institution to release copies of the video to the parent or eligible student.

In providing access to the video, the educational agency or institution must provide the parent of the student (or the student if the student is an eligible student) with the opportunity to inspect and review or "be informed of" the content of the video. If the educational agency or institution can reasonably redact or segregate out the portions of the video directly related to other students, without destroying the meaning of the record, then the educational agency or institution would be required to do so prior to providing the parent or eligible student with access. On the other hand, if redaction or segregation of the video cannot reasonably be accomplished, or if doing so would destroy the meaning of the record, then the parents of each student to whom the video directly relates (or the students themselves if they are eligible students) would have a right under FERPA to inspect and review or "be informed of" the entire record even though it also directly relates to other students.

For a fuller legal analysis and explanation of this issue, please see the 2017 Letter to Wachter.

4. If a video is an education record for multiple students, can the parent of one of the students (or the eligible student) receive a copy of the video?

While we do not advise on an educational agency's or institution's obligations under any state open records laws that may apply, we note that FERPA does not generally require an educational agency or institution to provide copies of education records to parents and eligible students[2]. That said, it would not violate FERPA for an educational agency or institution to non-consensually disclose to an eligible student or to his or her parents copies of education records that the eligible student or his or her parents otherwise would have the right to inspect and review under FERPA.

For a fuller legal analysis and explanation of this issue, please see the 2017 Letter to Wachter.

5. If redaction or segregation of an education record of multiple students can be reasonably accomplished without destroying the meaning of the education record, can educational agencies and institutions charge parents or eligible students for the costs of the redaction or segregation?

No. FERPA provides parents and eligible students with the right to inspect and review the student's education records, and nothing in the FERPA statute or regulations permits educational agencies and institutions to charge parents or eligible students for fees or costs associated with exercising that right.

If a school elects to provide a parent or eligible student with a copy of the education records, then the FERPA regulations (34 CFR § 99.11(a)) generally permit (with the exception noted below) the school to charge for the costs required to make the copy. FERPA regulations (34 CFR § 99.11(b)) also provide that the school may not charge a parent or eligible student for the costs to search for or retrieve the education records. We view the costs, if any, to the school of redacting, or segregating, education records of multiple students as being like the costs of search and retrieval that may not be charged to parents or eligible students, rather than like the costs for copies that generally may be charged to parents and eligible students. As noted above, if an educational agency or institution can reasonably redact or segregate out portions of an education record that is directly related to other students, without destroying the meaning of the record, then the educational agency or institution must do so and therefore cannot charge parents or eligible students for the costs associated with exercising their right to inspect and review such education records.

In contrast, parents and eligible students generally may be charged for the costs of making copies of education records precisely because FERPA generally does not require the school to provide them with such copies. Thus, where the redaction or segregation of education records of multiple students can be reasonably accomplished without destroying the meaning of the education records, nothing in FERPA permits educational agencies or institutions to charge parents or eligible students for the costs of making the required redactions or segregation. Please note that the FERPA regulations (34 CFR § 99.11(a)) similarly provide that if a fee for copies effectively prevents a parent or an eligible student from exercising the right to inspect and review his or her education records, an educational agency or institution would be required to provide copies without payment. Such cases would be limited to a parent or an eligible student providing evidence of the inability to pay for the copies due to financial hardship.

6. Does FERPA permit legal representatives of parents or eligible students to inspect and review videos with the parent or eligible student?

Yes. FERPA permits legal representatives of a parent or an eligible student to inspect and review videos with the parent or eligible student. While FERPA does not require educational agencies and institutions to allow parents or eligible students to bring their attorney or other legal

representative with them when they exercise their right to inspect and review the student's education records, nothing in FERPA prevents educational agencies and institutions from allowing parents or eligible students to bring their attorney or other legal representative with them when they exercise their right to inspect and review the student's education records under FERPA.

7. Does FERPA permit educational agencies and institutions turn over videos to the police upon request or following an incident that may warrant police involvement?

If the law enforcement unit of an educational agency or institution creates and maintains videos for a law enforcement purpose, then the videos would not be education records and FERPA would not prohibit the law enforcement unit of an educational agency or institution from disclosing the videos to the police. If the videos are education records, however, educational agencies and institutions may not turn over videos to the police upon request without having first either obtained the written consent of the parent or eligible student or determined that the conditions of an exception to the general requirement of consent have been met, such as if the disclosure is made in connection with a health or safety emergency (20 U.S.C. 1232g(b)(1)(I) and 34 CFR §§ 99.31(a)(10) and 99.36) or the law enforcement officer has presented the educational agency or institution with a judicial order or a lawfully issued subpoena (20 U.S.C. 1232g(b)(1)(J) and (b)(2) and 34 CFR § 99.31(a)(9)).

---

[1] The Individuals with Disabilities Education Act (IDEA) also contains privacy protections that apply to children with disabilities. 20 U.S.C. 1417(c) and 34 CFR §§ 300.610-300.626 and 34 CFR §§ 303.401-303.416. Under the IDEA, participating agencies must protect the personally identifiable information (PII), data, or records that are collected, maintained, or used by the participating agency. While the definition of "education record" under Part B of the IDEA cross-references the FERPA definition in 34 CFR § 99.3, the application of IDEA requirements may raise different questions.

[2] If circumstances effectively prevent the parent or eligible student from otherwise exercising their right to inspect and review the student's education records (e.g., if the parent lives outside of commuting distance to the school), then the educational agency or institution would be required to either provide a copy of the records or to make other arrangements for the parent or eligible student to inspect and review the records. 34 CFR § 99.10(d)

Audience:
K-12 School Officials

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF INNOVATION AND IMPROVEMENT

December 8, 2003

Ms. Shari A. Mamas
Staff Attorney
Education Law Center
1901 Law & Finance Bldg
429 Fourth Avenue
Pittsburgh, Pennsylvania 15219

Dear Ms. Mamas:

This is in response to your letter to this Office and also to the Office of Special Education Programs (OSEP) regarding the Family Educational Rights and Privacy Act (FERPA). Specifically, you ask whether FERPA prohibits a parent of a child with disabilities, or a professional working with a parent of a child with disabilities, from observing the child in a special or regular education classroom. I apologize for the delay in responding to your inquiry.

FERPA is a Federal law that protects a parent's privacy interest in his or her child's "education records." In particular, FERPA provides that an educational agency or institution may not have a policy or practice of denying parents the right to: inspect and review their children's education records; seek to amend education records; or consent to the disclosure of information from education records, except as provided by law. The term "education records" is defined as:

> [T]hose records, files, documents, and other materials, which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution.

20 U.S.C. § 1232g(a)(4). *See also* 34 CFR § 99.3 "Education records." Moreover, the records of a student which pertain to services provided to that student under the Individuals with Disabilities Education Act (IDEA) are "education records" under FERPA and are subject to the confidentiality provisions under IDEA (*see* 34 CFR § 300.560-300.576) and to all of the provisions of FERPA. (Part B of IDEA incorporates and cross-references FERPA.)

With regard to your specific question, FERPA does not specifically prohibit a parent or professional working with the parent from observing the parent' s child in the classroom. This is because FERPA would generally prohibit a teacher from disclosing information from a child's education records to other students in the classroom, as well as prohibit a teacher from disclosing information from a child's education records to the parents of another child who might be observing the classroom. Further, FERPA does not protect the confidentiality of information in general; rather, FERPA applies to the disclosure of tangible records and of information derived from tangible records.

With regard to your request that OSEP provide you with an opinion on whether IDEA "guarantees parents and their representatives a reasonable opportunity to observe their children's classrooms and proposed placement options," OSEP will contact you directly. I trust this is responsive to your inquiry.

Sincerely,

/s/

LeRoy S. Rooker
Director
Family Policy Compliance Office

Protecting Student Privacy While Using Online Educational Services: Model Terms of Service

About PTAC

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. PTAC provides timely information and updated guidance through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems. More PTAC information is available at https://studentprivacy.ed.gov.

PTAC welcomes input on this document and suggestions for future technical assistance resources relating to student privacy. Comments and suggestions can be sent to PrivacyTA@ed.gov.

Purpose of this Guidance

In February 2014, PTAC issued guidance titled *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*. This *Model Terms of Service* document is intended to further assist schools and school districts in implementing that guidance.

In a traditional contracting process, the buyer and seller mutually agree on a set of terms and then sign a contract reflecting those terms. However, many providers of online educational services and mobile applications (i.e., vendors, contractors, and other service providers) instead rely on a Terms of Service (TOS) agreement that requires a user to click to accept the agreement in order to access the service or application for the first time. These types of agreements are commonly referred to as "Click-Wrap" agreements. Once a user at the school or district clicks "I agree," these terms will likely govern what information the provider may collect from or about students, what they can do with that information, and with whom they may share it. Depending on the content, Click-Wrap agreements may lead to violations of the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), or other laws, as well as privacy best practices.

PTAC offers this guidance to schools and districts to help them evaluate potential TOS agreements, and to offer direction regarding terminology frequently used in these agreements. By understanding commonly used provisions, schools and districts will be better able to decide whether to consent to a Click-Wrap or other TOS agreement for online educational services and mobile applications. The best practice recommendations below may also assist providers by suggesting approaches that better protect student privacy.

Schools and districts should exercise diligence when reviewing TOS agreements and follow established school and district policies for evaluating and approving online educational services and mobile applications. This will help ensure that the service or application is inventoried and evaluated, supports the school's and district's

broader mission and goals, and that the TOS is legally appropriate and compatible with the school's and district's policies and procedures.

Terms of Service and Privacy

When negotiating a contract or evaluating a provider's TOS agreement, remember your school's or district's obligations regarding student privacy. Make sure the agreement explicitly describes how the provider may use and share student data.

The table below summarizes PTAC recommendations regarding key TOS provisions. The "GOOD!" column contains our best practice recommendations for TOS privacy provisions. If you see this language in your TOS, it is a positive indication that the provider is making a good faith effort to respect privacy. The "WARNING!" column contains provisions that represent poor privacy policy and may lead to violations of FERPA or other statutes. While these provisions are based on terms that may actually be used in providers' TOS or privacy policies, they are presented here solely as illustrations of the types of provisions to look for while performing your own reviews of a provider's privacy TOS. Actual TOS may have strong privacy protections that differ from those detailed below. As few TOS agreements will be worded exactly like the "GOOD!" or the "WARNING!" column, the final "Explanation" column provides context to help you interpret the rationale behind the provisions.

Privacy-Related Terms of Service Provisions

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
1	Definition of "Data"	"Data include all Personally Identifiable Information (PII) and other non-public information. Data include, but are not limited to, student data, metadata, and user content."	*Beware of provisions that limit the definition of protected data:* "Data only include user information knowingly provided in the course of using (this service)."	The definition of data should include a broad range of information to which providers may have access in order to ensure as much information as possible is protected in the agreement. Beware of provisions that narrowly define the "Data," "Student Information," or "Personally Identifiable Information" that will be protected.

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
2	Data De-Identification	"Provider may use de-identified Data for product development, research, or other purposes. De-identified Data will have all direct and indirect personal identifiers removed. This includes, but is not limited to, name, ID numbers, date of birth, demographic information, location information, and school ID. Furthermore, Provider agrees not to attempt to re-identify de-identified Data and not to transfer de-identified Data to any party unless that party agrees not to attempt re-identification."	*Beware of provisions that define de-identification narrowly (as only the removal of direct identifiers, such as names and ID numbers) or lack a commitment from Providers to not re-identify the Data:* "Provider may use de-identified Data for product development, research, or other purposes. De-identified Data will have all names and ID numbers removed."	There is nothing wrong with a provider using de-identified data for other purposes; privacy statutes, after all, govern PII, not de-identified data. But because it can be difficult to fully de-identify data, as a best practice, the agreement should prohibit re-identification and any future data transfers unless the transferee also agrees not to attempt re-identification. It is also a best practice to be specific about the de-identification process. De-identification typically requires more than just removing any obvious individual identifiers, as other demographic or contextual information can often be used to re-identify specific individuals. Retaining location and school information can also greatly increase the risk of re-identification.

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
3	Marketing and Advertising	"Provider will not use any Data to advertise or market to students or their parents. Advertising or marketing may be directed to the [School/District] only if student information is properly de-identified." *Or* "Data may not be used for any purpose other than the specific purpose(s) outlined in this Agreement." (*If this provision is present, check to make certain there is nothing else in the agreement that would allow marketing/advertising*).	"Provider may use Data to market or advertise to students or their parents."	The TOS should be clear that data and/or metadata may not be used to create user profiles for the purposes of targeting students or their parents for advertising and marketing, which could violate privacy laws.
4	Modification of Terms of Service	"Provider will not change how Data are collected, used, or shared under the terms of this Agreement in any way without advance notice to and consent from the [School/District]."	"Provider may modify the terms of this Agreement at any time without notice to or consent from the [School/District]." *Or* "Provider will only notify the [School/District] of material changes."	Schools/districts should maintain control of the data by preventing the provider from changing its TOS without the school's/district's consent. A provider that agrees to give notice of TOS changes is good; a provider that agrees not to change the TOS without consent is better.

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
5	Data Collection	"Provider will only collect Data necessary to fulfill its duties as outlined in this Agreement."	*An absence of a data collection restriction (see left) could potentially allow vendors to collect a wide array of student information.* *Also watch for:* "If user gains access through a third-party website *(such as a social networking site)*, personal information associated with that site may be collected."	If the agreement relates to FERPA-protected data, a provision like the one represented in the "GOOD!" column may be necessary. Including a provision that limits data collection to only what is necessary to fulfill the agreement is a best practice. Providers may view user access to their services through a third-party social networking site as an exception to established rules limiting data collection.
6	Data Use	"Provider will use Data only for the purpose of fulfilling its duties and providing services under this Agreement, and for improving services under this Agreement."	*Beware of any provision that contains the phrase:* "without providing notice to users."	Schools/districts should restrict data use to only the purposes outlined in the agreement. This will help schools/districts maintain control over the use of FERPA-protected student information and ensure appropriate data use.
7	Data Mining	"Provider is prohibited from mining Data for any purposes other than those agreed to by the parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited."	"Provider can mine or scan Data and user content for the purpose of advertising or marketing to students or their parents."	While data mining or scanning may sometimes be a necessary component of online services (e.g., for malware/spam detection or personalization tools), schools/districts should prohibit any mining or scanning for targeted advertising directed to students or their parents. Such provisions could lead to a violation of FERPA or the PPRA.

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
8	Data Sharing	"Data cannot be shared with any additional parties without prior written consent of the User except as required by law." *Or* "The [School/District] understands that Provider will rely on one or more subcontractors to perform services under this Agreement. Provider agrees to share the names of these subcontractors with User upon request. All subcontractors and successor entities of Provider will be subject to the terms of this Agreement."	"Provider may share information with one or more subcontractors without notice to User." *Or* "Where feasible, Provider will require third-party vendors to comply with these Terms of Service."	While it is perfectly acceptable for providers to use subcontractors, schools/districts should be made aware of these arrangements and subcontractors should be bound by the limitations in the TOS.
9	Data Transfer or Destruction	"Provider will ensure that all Data in its possession and in the possession of any subcontractors, or agents to which the Provider may have transferred Data, are destroyed or transferred to the [School/District] under the direction of the [School/District] when the Data are no longer needed for their specified purpose, at the request of the [School/District]."	*Beware of any provision that contains*: "maintain(s) the right to use Data or user content."	While FERPA does not specify that education records shared under some of its exceptions must be returned or destroyed at the end of the contract, it is a best practice to require this. Data return or destruction helps limit the amount of personal information available to third parties and prevent improper disclosure. This provision also helps schools/districts maintain control over the appropriate use and maintenance of FERPA-protected student information.

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
10	Rights and License in and to Data	"Parties agree that all rights, including all intellectual property rights, shall remain the exclusive property of the [School/District], and Provider has a limited, nonexclusive license solely for the purpose of performing its obligations as outlined in the Agreement. This Agreement does not give Provider any rights, implied or otherwise, to Data, content, or intellectual property, except as expressly stated in the Agreement. This includes the right to sell or trade Data."	"Providing Data or user content grants Provider an irrevocable right to license, distribute, transmit, or publicly display Data or user content."	Maintaining ownership of data to which the provider may have access allows schools/districts to retain control over the use and maintenance of FERPA-protected student information. The "GOOD!" provision will also protect against a provider selling information.
11	Access	"Any Data held by Provider will be made available to the [School/District] upon request by the [School/District]."	*Beware of any provision that would limit the school's or district's access to the Data held by Provider.*	FERPA requires schools/districts to make education records accessible to parents. A good contract will acknowledge the need to share student information with the school upon request in order to satisfy FERPA's parental access requirements. As a best practice, parental access to their children's data should be seamless.

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
12	Security Controls	"Provider will store and process Data in accordance with industry best practices. This includes appropriate administrative, physical, and technical safeguards to secure Data from unauthorized access, disclosure, and use. Provider will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Provider will also have a written incident response plan, to include prompt notification of the [School/District] in the event of a security or privacy incident, as well as best practices for responding to a breach of PII. Provider agrees to share its incident response plan upon request."	*The lack of a security controls provision, or inclusion of a provision that sets a lower standard for Provider's security of Data, would be a bad practice and potentially violate FERPA.*	Failure to provide adequate security to students' PII is not a best practice and could lead to a FERPA violation.

Resources

Materials below include links to PTAC and other resources that provide additional best practice recommendations and guidance relating to TOS agreements. Please note that these resources do not necessarily address particular legal requirements (including FERPA requirements) that your school or district needs to meet when collecting, storing, disseminating, or releasing education records to a provider. It is always a best practice to consult legal counsel to determine applicable federal, state, tribal, and local requirements prior to entering into contractual agreements with providers.

Department of Education Resources

- Privacy Technical Assistance Center, U.S. Department of Education: https://studentprivacy.ed.gov
- Privacy Technical Assistance Center, U.S. Department of Education, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* (2014): https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-eduacational-services-requirements-and-best
- Privacy Technical Assistance Center, U.S. Department of Education, *Written Agreement Checklist* (2012): https://studentprivacy.ed.gov/resources/written-agreement-checklist
- Family Policy Compliance Office, U.S. Department of Education: https://studentprivacy.ed.gov

Other Government Resources

- FTC: Bureau of Consumer Protection Business Center, *Complying with COPPA: Frequently Asked Questions:* https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions
- National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing* (2011): http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf