Safety, Privacy and Security in Technology: Fixing all your Problems in 20 Minutes*

*Disclaimer: May not fix all your problems

August 10, 2021

Frank Miller
Deputy Director
Student Privacy Policy Office

Ross Lemke
Director
Privacy Technical Assistance Center
Who are we?

The U.S. Department of Education’s Student Privacy Policy Office (SPPO) is responsible for the administration and enforcement of federal laws, relating to the privacy of students’ education records, and for the provision of technical assistance on student privacy issues for the broader education community.
What is PTAC?

• The Department’s Privacy Technical Assistance Center (PTAC), located within the Student Privacy Policy Office, was established in 2010 as a “one-stop” resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level data systems and other uses of student data. PTAC’s primary role is the provision of the following services:
  • operating a Student Privacy Help Desk, offering assistance on complex student privacy issues to the education community via phone or email;
  • conducting technical assistance site visits to SEAs and LEAs; and
  • hosting privacy-focused regional meetings and lessons learned forums for education stakeholders
  • developing privacy and security training materials for states and districts;
  • issuing privacy and security best practice recommendations, including issue briefs and checklists
Pop Quiz!

1. FERPA only applies to schools that receive federal education funds.  
   T  F

2. Once a student turns 18, the school can’t share education records with the parents.  
   T  F

3. The Family Educational Rights and Privacy Act (FERPA) is the only privacy law that the Student Privacy Policy Office administers  
   T  F
How did you do?

• FERPA is hard!
• Most audiences score 40% on our FERPA 101 pretest.
• Many FERPA violations stem from a lack of understanding, or worse, a partial understanding of FERPA.
• The Student Privacy Policy Office has over 200 resources to help with privacy and security issues.
A Parent Guide to the Family Educational Rights and Privacy Act

SPPO-21-04

A Parent Guide to the Family Educational Rights and Privacy Act (FERPA)

Other than statutory and regulatory requirements included in the document, the contents of this guidance do not have the force and effect of law and are not meant to bind the public. This document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.

The Family Educational Rights and Privacy Act or FERPA (20 U.S.C. § 1232g; 34 CFR Part 99) provides certain rights for parents regarding their children’s education records. FERPA gives these rights to custodial and noncustodial parents alike, unless there is a court order, legally binding document, or State law that specifically provides to the contrary. When a student reaches 18 years of age or attends an institution of postsecondary education at any age, he or she becomes an “eligible student,” and all rights under FERPA transfer from the parent to the student. Given the target audience for this document is parents, this guide is intended to discuss parents’ rights under FERPA. Under FERPA, the term “parent” means a parent of a student and includes a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or a guardian. A companion document discussing eligible students’ rights under FERPA is available on our website at https://studentprivacy.ed.gov/resources/ferpa-general-guidance-students.

FERPA is a Federal law that is administered by the Student Privacy Policy Office (SPPO) in the U.S. Department of Education (Department). FERPA protects “education records,” which are generally defined as records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution. An “educational agency or institution,” herein after referred to as a “school,” generally means a school district, a public elementary or secondary school, or an institution of postsecondary
Protection of Pupil Rights Amendment (PPRA)

UNITED STATES DEPARTMENT OF EDUCATION
STUDENT PRIVACY POLICY OFFICE

SPPO-21-01

Protection of Pupil Rights Amendment (PPRA)

Other than statutory and regulatory requirements included in the document, the contents of this 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.

Rights of Parents under PPRA

PPRA (20 U.S.C. § 1232h, 34 CFR Part 98) affords parents of students certain rights regarding, among other things, participation in surveys, the collection and use of information for marketing purposes, and certain physical exams. These include, but are not limited to, the right to:

- Consent before students are required to submit to a survey that concerns one or more of the following eight protected areas (protected information survey) if the survey is funded as part of a program administered by the U.S. Department of Education (Department) (applicable program) –
  1. Political affiliations or beliefs of the student or student’s parent;
  2. Mental or psychological problems of the student or student’s family;
  3. Sex behavior or attitudes;
  4. Illegal, anti-social, self-incriminating, or demeaning behavior;
  5. Critical appraisals of others with whom respondents have close family relationships;
  6. Legally recognized privileged or analogous relationships, such as with lawyers, doctors, or ministers;
  7. Religious practices, affiliations, or beliefs of the student or student’s parent; or
  8. Income, other than as required by law to determine program eligibility.

- Receive notice and an opportunity to opt a student out of –
Videos

Guidance Videos

These short videos are intended to provide guidance on specific topics surrounding student privacy, or have been produced as easy-to-use companions to existing guidance documents. New videos are added periodically.

All Audiences

All Topics

Apply

Clear

What Happens When I File a Complaint?

The Family Educational Rights and Privacy Act, or FERPA, provides certain rights for parents and eligible students around student education records.

Topics: Family Educational Rights Privacy Act (FERPA)

FERPA’s Complaint Process Explained

The Family Educational Rights and Privacy Act, or FERPA, provides certain rights for parents and eligible students around student education records.

Topics: Family Educational Rights Privacy Act (FERPA)

Introduction to Blockchains for Educators

Introduction to Blockchains for Educators is the first in a series of videos intended to introduce the technology behind blockchains and provide in

Topics: Data Governance, Data Sharing, Disclosures Avoidance, Family Educational Rights Privacy Act (FERPA)

School Volunteers and FERPA

Email and Student Privacy

What Parents Need to Know about their Student’s Data
Webinars

Recorded Webinars

This section houses recordings of the various webinars that have been conducted on various aspects of student privacy. These webinars explore topics in depth or have been conducted to support previously released guidance documents. New recordings are posted periodically as new webinars are presented.

- FERPA and Virtual Learning during COVID-19 (Webinar Recording)
  - Webinar recording for “FERPA and Virtual Learning during the COVID-19” presentation. This webinar is intended to provide information on privacy.
  - Topics: FERPA, Educational Rights and Privacy Act (FERPA)

- Colleges and the 2020 Census – Webinar
  - This webinar accompanies the guidance document on the 2020 Census and Colleges. This presentation provides background information on reporting requirements.
  - Topics: Data Sharing, Disclosure Avoidance

- Protecting Student Privacy While Using Online Educational Services – March 2014
  - This webinar provides an overview of the guidance document entitled “Protecting Student Privacy While Using Online Educational Services.”
  - Topics: Data Sharing, Educational Rights and Privacy Act (FERPA), Security Best Practices


- Disclosure Avoidance and Limiting Access to PII – November 2012

- Intersection of FERPA and IDEA Confidentiality Provisions – March 2012
Training

Online Training Modules

**We appreciate your patience as we updated and enhanced our FERPA Training modules! Due to the high demand for training, we are opening up access to the new system early in order to meet our fantastic education community’s needs during our final testing phase. Sign up for the FERPA Newsletter to be up to date on student privacy resources.**

[Image of Online Training Modules]

- **FERPA 101: For Local Education Agencies**
  - This interactive computer-based training course introduces learners to the basics of the Family Educational Rights and Privacy Act (FERPA) as it applies to Colleges, Universities and other Post-secondary Institutions.

- **FERPA 201: Data Sharing under FERPA**
  - Training focused on the intricacies of sharing data in compliance with FERPA requirements.

- **FERPA 301: For Local Education Agencies**
  - FERPA training focused on K-12 schools, districts and local education agencies.
**Pop Quiz 1!**

1. You must have a data sharing agreement in place to disclose PII from education records to a vendor without consent of parents or eligible students.  
   - **T/F**  
   - **T**

2. If a software vendor were to improperly disclose PII from education records to another vendor without consent of the parents, those parents can file a FERPA complaint against that vendor.  
   - **T/F**  
   - **F**
Technology is here to stay

• Education technology can do some great things.

• As education professionals it is our responsibility to ensure that these tools are used appropriately.

• The first step in this is to develop a policy on the use of apps in the classroom.
Ed Tech Resources PTAC

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
Ed Tech Resources

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
Pop Quiz 2!

1. Schools must always obtain consent to disclose information to School Resource Officers (SROs).
   T   F

2. Student health records maintained by the school nurse are not education records.
   T   F
SRO and School Safety Resources

School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA)

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.

Introduction

School officials routinely seek to balance the interests of safety and privacy for students. While the Family Educational Rights and Privacy Act (FERPA) generally requires written parent or “eligible student” consent before an educational agency (district) or institution (school) discloses student education records and the personally identifiable information (PII) contained therein, FERPA gives schools and districts flexibility to disclose PII, under certain limited circumstances, in order to maintain school safety. The purpose of this guidance is to address questions about how FERPA applies to schools’ and districts’ disclosures of PII from student education records to school security units, outside law enforcement entities, School Resource Officers (SROs), and other schools. While the information in this guidance is applicable to all educational agencies and institutions that receive funds under any program administered by the Secretary of the U.S. Department of Education (Department), the discussion is generally focused on health or safety emergencies faced by public elementary and secondary schools.
Covid-19 Resources

FERPA and Virtual Learning during COVID-19 (Webinar Recording)

FERPA & VIRTUAL LEARNING DURING COVID-19
March 30, 2020

Kala Shah Surpremant
Acting Director,
Student Privacy Policy Office
U.S. Department of Education
Pop Quiz 3!

1. FERPA does not require you to use specific technology to protect IT data systems?
   - T
   - F

2. All FERPA violations are Data Breaches.
   - T
   - F

Computers and the internet are integral to our lives, from online shopping to paying our taxes. Schools use computer systems to provide better learning environments for students, reduce administrative overhead, and give parents more visibility into their children’s education. However, schools, like every other organization, face continued challenges protecting the data in their systems from breaches.

This document aims to provide parents of K-12 students information to help understand what it means when your school has a data breach, as well as provide tools and best practices to help navigate the sometimes confusing process of protecting your children’s data in the event of a breach.

What is a Data Breach?

Data breaches come in many different forms, from cyber criminals breaking into school data systems and stealing sensitive data about students or employees, to accidental disclosures due to errors or misconfigurations. For the purposes of this document, a data breach can be understood as any circumstance where a school’s student data system is improperly accessed, compromised, or disclosed to a third party.

What about FERPA?

The Family Educational Rights and Privacy Act, commonly referred to as FERPA, is a federal law that, among other things, protects the privacy of personally identifiable information (PII) from education records. While FERPA does not explicitly address “data breaches,” it generally prohibits the disclosure of PII from education records without prior written consent from the parent or eligible student (34 CFR § 99.30), unless one of FERPA’s exceptions to the written consent requirement applies. FERPA does not require a school to notify a parent that information from their child’s education records was stolen or
Data Breach Response Training Kits.

Password District Data Breach Exercise

[District Name]

[Date]

Click icon to add picture

[Logo]
Data Breach Response Training Kits

• Tabletop exercise that simulates a data breach scenario between organizations that share student data.

• Intended to put you in the shoes of critical decision-makers who have just experienced a data breach.

• Four scenarios available: Password, Dual Enrollment, Malicious Software, Postsecondary.
Student Privacy Listserv

Join the Student Privacy Listserv

The U.S. Department of Education is releasing new material all the time. This material comes in the form of Best Practices material from the Privacy Technical Assistance Center and policy guidance and letters from the Student Privacy and Policy Office. To stay abreast of these developments, please join our Student Privacy listserv.

FEATURED RESOURCES

FERPA and the Coronavirus Disease 2019 (COVID-19)

The purpose of this guidance is to answer questions that school officials may have had concerning the disclosure of personally identifiable information from students’ education records to outside entities when addressing the Coronavirus.
CONTACT INFORMATION

United States Department of Education, Student Privacy Policy Office

(855) 249-3072
(202) 260-3887
privacyTA@ed.gov
https://studentprivacy.ed.gov