PTAC Supporting YOUR Data Privacy Work

April 25, 2022

Ross Lemke
Director
Privacy Technical Assistance Center
Disclaimer

This content was produced by the U.S. Department of Education’s Student Privacy Policy Office through its Privacy Technical Assistance Center for the purposes of this presentation. This presentation is provided for informational purposes only. Nothing in this presentation constitutes official policy or guidance from the U.S. Department of Education. Official policy and guidance can be found on our website at https://studentprivacy.ed.gov/.
Who do we support?

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. FERPA is the only privacy law that the Student Privacy and 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.
https://studentprivacy.ed.gov

Student Privacy at the U.S. Department of Education

The U.S. Department of Education is committed to protecting student privacy. We administer and enforce student privacy laws such as the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA). In addition, we provide technical assistance to help schools and school districts safeguard information about students.

To learn more about federal student privacy laws and your rights please see the short video to the right or explore these other resources:

- FERPA General Guidance for (Newly updated) Parents or Students
- PPRA General Guidance
- Frequently Asked Questions on Photos and Videos
- FERPA Regulations
- PPRA Regulations
A Parent Guide to the Family Educational Rights and Privacy Act

United States Department of Education, Student Privacy Policy Office

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...
FERPA’s Complaint Process Explained
What Happens When I File a Complaint?
MALWARE IS EVERYWHERE

IF YOU DON'T TRUST THE LINK, DON'T CLICK IT!

For more information, visit the U.S. Department of Education's Student Privacy Policy Office https://studentprivacy.ed.gov

PERSONALLY IDENTIFIABLE INFORMATION

- NAME
- MOTHER’S MAIDEN NAME
- HOME ADDRESS
- DATE OF BIRTH
- PLACE OF BIRTH
- SOCIAL SECURITY NUMBER
- NAME OF PARENTS
- FINGERPRINT

For more information, visit the U.S. Department of Education's Student Privacy Policy Office https://studentprivacy.ed.gov

BEFORE YOU SHARE THAT STUDENT RECORD...

STOP!
THINK!

FERPA!

REMEMBER IT'S UP TO YOU TO KEEP STUDENT DATA SAFE!

For more information, visit the U.S. Department of Education's Student Privacy Policy Office https://studentprivacy.ed.gov
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 PTAC Newsletter to be up to date on student privacy resources.”

United States Department of Education, Student Privacy Policy Office
Pop Quiz!

1. Schools are always free to administer surveys to students without the consent of parents.

2. The Protection of Pupil Rights Amendment expired when the Elementary and Secondary Education Act was Reauthorized in 2015
A Parent’s Guide to PPRA

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 –
PPRA Video
Pop Quiz!

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

2. If a software vendor were improperly disclose PII from education records to a vendor without consent of parents, those parents can file a FERPA complaint against that vendor.  
   - T  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

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
Ed Tech Resources

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
Pop Quiz!

1. Schools must always obtain consent to disclose information to law enforcement or health officials. 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](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 Surpreenat
Acting Director,
Student Privacy Policy Office
U.S. Department of Education
Pop Quiz!

1. SEAs, Districts and IHEs are permitted to share data with third party researchers using the research exception.  
   - T  
   - F

2. Institutional Review Board approval of a project means the project is permissible under FERPA.  
   - T  
   - F
FERPA and Researchers

• Education data, when used appropriately, can provide insights that can improve the outcomes for students

• When student data is shared with third parties, the law requires schools and education agencies to ensure that data is
  • protected and
  • not redisclosed without permission
FERPA and Researchers

- FERPA exceptions are *permissive*
- Nothing in FERPA states schools or education agencies MUST share the data
- As a school or education agency it is incumbent on you to ensure that the data sharing is compliant with FERPA and other state laws
- Some research projects might not fit an exception and in that case, consent may be required
Tips for Education Agencies

• FERPA exceptions are *permissive* – this bears repeating

• Nothing in FERPA states schools or education agencies MUST share the data

• As a school or education agency it is incumbent on you to ensure that the data sharing is compliant with FERPA and other state laws

• Some research projects might not fit an exception and in that case, consent may be required
Tips for Researchers

• Only request the data you *really* need
• You MUST protect the data you hold
• YOUR FUTURE RESEARCH MAY DEPEND ON BEING A GOOD STEWARD
• PTAC is a resource you can go to for help
Resources for Researchers

Written Agreement Checklist

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

The purpose of this document is to summarize the requirements for the written agreements under the studies exception and the audit or evaluation exception as specified in the Family Educational Rights and Privacy Act (FERPA). The FERPA regulations on the studies exception requires that the educational agency or institution or the state or local education authority or agency headed by an official listed in 34 CFR §99.31(a)(3) execute a written agreement with the organization conducting the study when disclosing personally identifiable information from education records without consent (see 34 CFR §99.31(a)(6)(iii)(C)). The FERPA regulations on the audit or evaluation exception require that the state or local education authority or agency headed by an official listed in 34 CFR §99.31(a)(3) must use a written agreement to designate any authorized representative other than an employee (see 34 CFR §99.35(a)(3)). The mandatory elements of that agreement vary slightly between the two exceptions. The following checklist delineates the minimum requirements under the studies and the audit or evaluation exceptions. The list of the mandatory elements is followed by best practice suggestions that may help to further enhance the transparency and effectiveness of the agreements.
Pop Quiz!

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
WE HAVE DATA SECURITY BEST PRACTICES DOWN HERE
A Parent’s Guide for Understanding
K-12 School Data Breaches

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.
Trends in Cybersecurity

• Increase in ransomware related incidents
  • New attack paradigms
• Increase in the number of vendor related incidents
• Districts till have a ton of old or unpatched software
• IoT devices remain an issue
• Users remain your weakest link
<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Landline number</td>
<td>Blackened</td>
</tr>
<tr>
<td>Mobile phone</td>
<td>Blackened</td>
</tr>
<tr>
<td>Email</td>
<td>Blackened</td>
</tr>
<tr>
<td>Relatives</td>
<td>Blackened</td>
</tr>
</tbody>
</table>

View larger map
How Attackers Exploit this Info

• Start high level and look at his papers, slides and emails to spot weaknesses in the enterprise

• Target with spear phishing / whaling attacks to phone, email, SMS

• Impersonation attacks against staff at the school

• Leverage friends & colleagues names to elicit action or shift focus to them

• Failing that, there’s always blackmail, intimidation, coercion and threats
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.
The CPO Network

• In 2021 PTAC create the Chief Privacy Officer Network to provide CPOs with an opportunity to engage with their peers around student data privacy or security challenges, share promising best practices and resources, and identify potential areas of future collaboration.

• The CPO Network is not intended to be an advisory and/or policy group for the Department, nor will the Network operate as a platform for the Department to solicit recommendations or advice from the field.

• In addition, the Department will not be using the Network for compliance purposes.
The CPO Network

• The Network meets quarterly with the next person to be held along with EIMAC in Jacksonville next month

• PTAC hosts monthly office hours with CPO Network members to discuss whatever issue or concern is on the members minds
  • Incident response
  • Cybersecurity insurance
Student Privacy Helpdesk

- Remember – FERPA is hard
- When in doubt call (855) 249-3072
- privacyTA@ed.gov
A glimpse into the helpdesk

Bob, Tommy and Joe are ecstatic that their favorite NFL team, the Philadelphia Eagles have won the Superbowl. They go to the local bar to celebrate and wind up celebrating too much. Inebriated, they return to campus and stumble around drunkenly trying to find their dorm rooms.

While they are doing nothing violent, their behavior violates the school’s alcohol policy and several students complain about the incident. Campus administration reviews the surveillance video and clearly can see the three fans and their celebrations. The administration confirms that they have violated the school’s alcohol policy and put the three students on probation. Tommy is a basketball player and this probation is preventing him from competing in this weekend’s big game.
A glimpse into the helpdesk

1. The student newspaper, doing a story on discipline incidents for student athletes and submits a public records request for the video. Must you comply with the public records request?

2. Joe comes from an affluent family that donates a lot of money to the university. They ask for the university to destroy the video so it doesn’t damage Joe’s future political career. How would you handle the request from the parents to destroy the video?

3. Bob has no recollection of the evening and requests to come in and view the video so he can be sure that it was him. Do you have to comply with the request?
So, Are Videos Education Records?
PTAC Being Asked this Question, Circa 2017
PTAC Being Asked this Question, Circa 2018

YOU GET AN ANSWER,
YOU GET AN ANSWER

YOU ALL GET AN ANSWER
When are Videos and Photos Education Records

When they are directly related to a student. Which means they are:

• Used for disciplinary action or other official purposes
• Depictions of activities that:
  1. Resulted in disciplinary action
  2. Shows a violation of the law
  3. Shows an occurrence of student injury, attack, illness or health emergency
• Intent to make a specific student the subject
• Audio or visual record contains content that includes PII from a student’s education record.
When Videos and Photos are NOT Education Records

- Students in the background
- Photos or videos without a focus on a specific student
- Records maintained by a law enforcement unit of an educational agency or institution for a law enforcement purpose
  - however, if unit provides a copy to the school, that copy may become an education record
Videos and Photos that are Records of Multiple Students

• A video can be the education record of multiple student (e.g. fights)

• In such an instance, educational agencies and institutions are required to allow a parent or eligible student, upon request, the opportunity to inspect and review the record without the consent of the other parent/eligible student.

  a) Prior to providing access institutions are required to redact or segregate when reasonable if it does not destroy the meaning of the video

  b) Schools cannot charge for the redaction or segregation

  c) Copies are allowed but not required
PTAC Service Offerings

• FERPA 101 training
• Data sharing training
• FERPA 201 training
• Basic and advanced data security training
• Data breach table tops
• Disclosure Avoidance training
• Hack-a-thon – NEW!
• Many more
Hack-a-thon

- Participants take off their white hat and assume the role of the adversary
- Virtual lab environment consists of a self contained education ecosystem including an SIS, district website and employee workstation
- Participants learn first hand what the bad guys look for while trying to crack into district networks
Coming Attractions

• Summer Webinar Series
  • How to build an incident response plan
  • FERPA 101
  • TBD

• Researcher workshop at the AIR conference

• Several state site visits and conferences (maybe you are next?)

• National virtual site visit in the August/September time frame
CONTACT INFORMATION

United States Department of Education,
Student Privacy Policy Office

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