Protecting Student Privacy While Using Online Educational Services

An Overview of Recent Department of Education Guidance

March 13, 2014

Michael Hawes
Statistical Privacy Advisor
U.S. Department of Education

Baron Rodriguez
Director
Privacy Technical Assistance Center

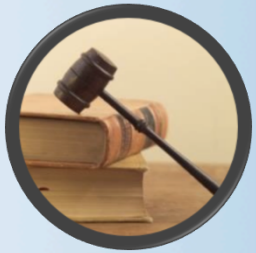
Webinar Logistics

- Phone lines will be muted

- Interactive polls

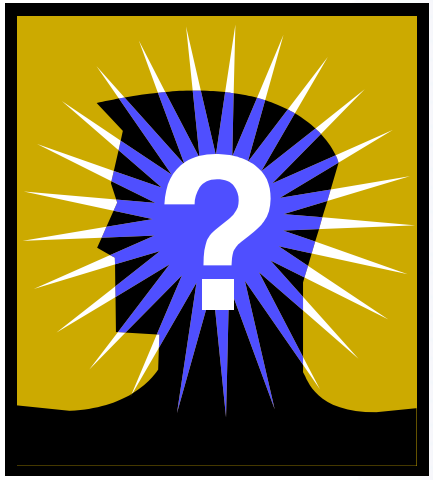
- The recording of this webinar will be made available on the PTAC website: https://studentprivacy.ed.gov

- Legal citations are available within the new guidance document



Questions

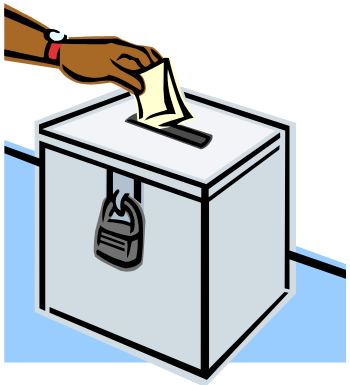
- Please type your questions in the chat box in the lower right hand corner of the webinar window



Poll: Who is in the Audience?

Please indicate which sector you represent:

A) K-12 Administration
B) K-12 Faculty
C) Post-Secondary Administration or Faculty
D) Education Technology Industry
E) Other (e.g., parent/student, non-profit org., etc.)



Overview

- The changing landscape of education technology in schools
- The U.S. Department of Education's role in protecting student privacy
- Legal protections for students' information used in online educational services
  - How FERPA and PPRA protect student information used in online educational services
  - Other laws to consider
- Beyond compliance: best practices for protecting student privacy

"We must provide our schools, teachers and students cutting-edge learning tools. And we must protect our children's privacy. We can and must accomplish both goals..."

U.S. Secretary of Education Arne Duncan
February 24, 2014

Use of Education Technology in Schools

- Student Information Systems
- Productivity applications
- Educational applications
- Fundamental school services

Online Educational Services

This guidance relates to the subset of educational services that are:

- Computer software, mobile applications (apps), or web-based tools;
- Provided by a third-party to a school or district;
- Accessed via the Internet by students and/or parents; AND
- Used as part of a school activity.

This guidance does not cover online services or social media used in a personal capacity, nor does it apply to services used by a school or district that are not accessed by parents or students.

The Challenge of Online Educational Services

- Schools and districts are increasingly contracting out school functions
- We have new types of data, and much more of it!
- Many online services do not utilize the traditional 2-party written contractual business model
- Increasing concern about the commercialization of personal information and behavioral marketing
- We need to use that data effectively and appropriately, and still protect students' privacy

The U.S. Department of Education's Role in Protecting Student Privacy

- Administering and enforcing federal laws governing the privacy of student information
  - Family Educational Rights and Privacy Act (FERPA)
  - Protection of Pupil Rights Amendment (PPRA)
- Raising awareness of privacy challenges
- Providing technical assistance to schools, districts, and states
- Promoting privacy & security best practices

Poll: FERPA Awareness

Please rate your familiarity with FERPA:

A) "FERPA, what's FERPA?"

B) I know enough to be dangerous

C) You could add me to your national cadre of experts on FERPA: I'm an expert

Family Educational Rights and Privacy Act (FERPA)

- Gives parents (and eligible students) the right to access and seek to amend their children's education records
- Protects personally identifiable information (PII) from education records from unauthorized disclosure
- Requirement for written consent before sharing PII – unless an exception applies

But Wait! There are Exceptions!

Two of FERPA's exceptions to the parental consent requirement are most relevant when using education technology:

- Directory information exception
- School official exception

There are many other FERPA exceptions.

Directory Information Exception

- Students don't attend school anonymously
- Allows schools to release certain information without consent. A few examples:
  - name, address, telephone listing, electronic mail address;
  - date and place of birth;
  - photographs;
  - weight and height of athletes;
  - degrees & awards received.

Directory Information Exception

- Common uses:
  - Yearbooks
  - Concert programs
  - Telephone directories

- Remember that parents have a right to opt-out

School Official Exception

- Schools or LEAs can use the School Official exception to disclose education records to a third party provider (TPP) if the TPP:
  - Performs a service/function for the school/district for which it would otherwise use its own employees
  - Is under the direct control of the school/district with regard to the use/maintenance of the education records
  - Uses education data in a manner consistent with the definition of the "school official with a legitimate educational interest," specified in the school/LEA's annual notification of rights under FERPA
  - Does not re-disclose or use education data for unauthorized purposes

Poll: PPRA Awareness

Please rate your familiarity with PPRA:

A) (Yawn) I know all about it

B) I've worked with it, but only in regard to the survey provisions

C) I have limited knowledge about PPRA

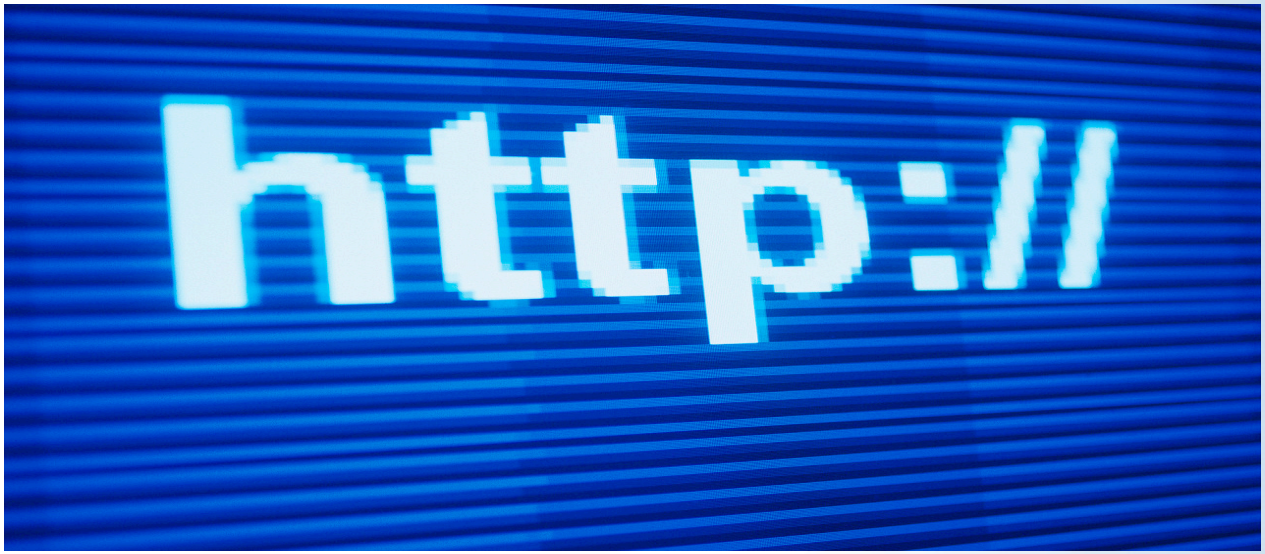
D) Oh yes, that stands for "Pen Pal Research Association," right?

Protection of Pupil Rights Amendment (PPRA)

- Amended in 2001 with No Child Left Behind Act
- Mostly known for provisions dealing with surveys in K-12
- Includes limitations on using personal information collected from students for marketing
- Parental notification and opportunity to opt out may be required
- Development of policies in conjunction with parents may be required
- However … a significant exception for “educational products or services”

Question 1:

Is student information used in online educational services protected by FERPA?



Is student information used in online educational services protected by FERPA?

It depends!

Some data used in online educational services is protected by FERPA.

Other data may not be.

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 is implicated.

Question 2:

What does FERPA require if PII from students' education records is disclosed to a provider?

What does FERPA require if PII is disclosed to a provider?

- Parental consent for the disclosure; OR
- Disclosure under one of FERPA's exceptions to the consent requirement. Typically, either:
  - Directory Information exception
    - Remember parents' right to "opt-out"
  - School Official exception
    - Annual FERPA notice
    - Direct control
    - Use for authorized purposes only
    - Limitation on re-disclosure
    - *Remember parents' right to access their student's education records*

Question 3:

Under FERPA and PPRA, are providers limited in what they can do with the student information they collect or receive?

Are providers limited in what they can do with the student information they collect or receive?

If PII is disclosed under the Directory Information exception:

- No limitations

If PII is disclosed under the School Official exception:

- PII from education records may only be used for the specific purpose for which it was disclosed
- TPPs may not sell or share the PII, or use it for any other purpose except as directed by the school/district and as permitted by FERPA

When personal information is collected from a student, the PPRA may also apply!

- *PPRA places some limitations on the use of personal information collected from students for marketing*

Are providers limited in what they can do with the student information they collect or receive?

Remember, schools and districts have an important role in protecting student privacy.

Additional limitations and restrictions (beyond what FERPA, PPRA, and other laws require) may be written into the agreement between the school/district and the provider!

Question 4:

What about metadata? Are there restrictions on what providers can do with metadata about students' interactions with their services?

What about metadata?

"Metadata" are pieces of information that provide meaning and context to other data being collected, for example:

- Activity date and time
- Number of attempts
- How long the mouse hovered before clicking an answer

Metadata that have been stripped of all direct and indirect identifiers are not protected under FERPA.

(NOTE: School name and other geographic information can be indirect identifiers in student data.)

Properly de-identified metadata may be used by providers for other purposes (unless prohibited by other laws or by their agreement with the school/district).

Other Laws to Consider

- Children's Online Privacy and Protection Act (COPPA)
  - Applies to commercial Web sites and online services directed to children under age 13, and those Web sites and services with actual knowledge that they have collected personal information from children
  - Schools may exercise consent on behalf of parents in certain, limited circumstances *(e.g., when it is for the use/benefit of the school and there is no other commercial purpose)*
  - Administered by the Federal Trade Commission
  - See http://www.business.ftc.gov/privacy-and-security/childrens-privacy for more information
- State, Tribal, or Local Laws

Best Practices for Protecting Student Privacy

- **Maintain awareness of other relevant laws**
- Be aware of which online educational services are currently being used in your district
- Have policies and procedures to evaluate and approve proposed educational services
- When possible, use a written contract or legal agreement
- Be transparent with parents and students
- Consider that parental consent may be appropriate

Best Practices for Protecting Student Privacy

- Maintain awareness of other relevant laws
- **Be aware of which online educational services are currently being used in your district**
- Have policies and procedures to evaluate and approve proposed educational services
- When possible, use a written contract or legal agreement
- Be transparent with parents and students
- Consider that parental consent may be appropriate

Best Practices for Protecting Student Privacy

- Maintain awareness of other relevant laws
- Be aware of which online educational services are currently being used in your district
- **Have policies and procedures to evaluate and approve proposed educational services**
- When possible, use a written contract or legal agreement
- Be transparent with parents and students
- Consider that parental consent may be appropriate

Question 5:

Can individual teachers sign up for free (or “freemium”) education services?

Using free educational services

Remember the FERPA's requirements for schools and districts disclosing PII under the school official exception

- Direct control
- Consistency with annual FERPA notice provisions
- Authorized use
- limits on re-disclosure

These services may also introduce security vulnerabilities into your school networks.

It is a best practice to establish district/school level policies governing use of free services, and to train teachers and staff accordingly.

Best Practices for Protecting Student Privacy

- Maintain awareness of other relevant laws
- Be aware of which online educational services are currently being used in your district
- Have policies and procedures to evaluate and approve proposed educational services
- **When possible, use a written contract or legal agreement**
- Be transparent with parents and students
- Consider that parental consent may be appropriate

Best Practices for Protecting Student Privacy

- Maintain awareness of other relevant laws
- Be aware of which online educational services are currently being used in your district
- Have policies and procedures to evaluate and approve proposed educational services
- When possible, use a written contract or legal agreement
- **Be transparent with parents and students**
- Consider that parental consent may be appropriate

Best Practices for Protecting Student Privacy

- Maintain awareness of other relevant laws
- Be aware of which online educational services are currently being used in your district
- Have policies and procedures to evaluate and approve proposed educational services
- When possible, use a written contract or legal agreement
- Be transparent with parents and students
- **Consider that parental consent may be appropriate**

Question 6:

What provisions should be in a school's or district's contract with a provider?

Best Practices for Contract Provisions for Online Educational Services

- Security and data stewardship provisions
- Data collection provisions
- Data use, retention, disclosure, and destruction provisions
- Data access provisions
- Modification, duration, and termination provisions
- Indemnification and warranty provisions

Question 7:

What about online educational services that use “click-wrap” agreements instead of traditional contracts?

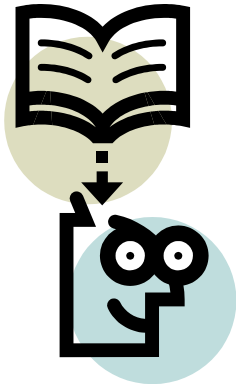
What to look for in “click-wrap” agreements

When reviewing “click-wrap” agreements, schools and districts should also:

- Check amendment provisions
- Print (or save) the Terms of Service
- Specify authority to accept the Terms of Service

Read the Guidance Document

https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-and-best



Resources

- Family Policy Compliance Office, U.S. Department of Education, Model Notice for Directory Information
- PTAC Cloud Computing Best Practices
- Federal Trade Commission Resources on COPPA and Children's Privacy
- National Institute of Standards and Technology, Cloud Computing Guidelines for Managing Security and Privacy

Questions

- Please type your questions in the chat box in the lower right corner of the webinar screen

Contact Information

Privacy Technical Assistance Center

Telephone: (855) 249-3072

Email: privacyTA@ed.gov

FAX: (855) 249-3073

Website: https://studentprivacy.ed.gov