



Working with Online Educational Service Providers and Apps

WISEdata Conference

Ross Lemke

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/>.



Should you be here?

- Does your school use Educational Technology on in your school?
- Do you know every app your teachers are using?
- Do you know what student data is getting put into those apps?
- Do you like presentations with memes?

Summary of Today's Discussion

Background and Regulatory Requirements

- The changing landscape of education technology on campus
- Legal protections for students' information used in online educational services
 - How FERPA and PPRA protect student information used in online educational services

"Musts"

Best Practices

- Beyond compliance: best practices for protecting student privacy
- Resources for developing your own policy on third party applications

"Shoulds"

Online Educational Services

Today's guidance relates to the subset of education services that are:

- Computer software, **mobile applications (apps)**, or web-based tools;
- Provided by a third-party to an educational institution;
- 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 institution that are not accessed by students.*

The Challenge of Online Educational Services

- Postsecondary institutions 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.



PTAC's Favorite Line from EDTech Vendors

- "Our Software is FERPA Compliant. We're School Officials."



Things that don't Exist

- Unicorns
- Dragons
- Official Department of Education FERPA seal of approval



How does the vendor get the data?

- Under FERPA, to share data with a vendor it has to happen under two ways:
 - Consent
 - Consent must be signed and dated and must:
 - Specify the records that may be disclosed
 - State purpose of disclosure; and
 - Identify party or class of parties to whom disclosure may be made
 - One of the exceptions under FERPA:
 - Directory Information Exception
 - School Official Exception

Directory Information

- Information in a student's education records that would not generally be considered harmful or an invasion of privacy if disclosed.
- This may include: Name, address, phone number, grade, photograph....
- Each institution determines their own directory policy which includes an opt out provision.
- Some institutions use a limited directory information policy that restricts who can receive directory data.

School Official Exception

- Schools may disclose PII from education records without consent if the disclosure is to other school officials within the school, including faculty, whom the school has determined to have legitimate educational interest.
- Schools may outsource institutional services or functions that involve the disclosure of education records to contractors, consultants, teaching assistants, or other third parties provided certain conditions are met.

Conditions for Outsourcing

- Performs an institutional service or function for which the agency or institution would otherwise use its employees;
- Is under the direct control of the agency or institution with respect to the use and maintenance of education records;
- PII from education records may be used only for the purposes for which the disclosure was made, and may not be redisclosed without the authorization of the educational agency or institution and in compliance with FERPA;
- Meets the criteria specified in the school, LEA, or institution's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records.

Annual Notice

- Each institution has an annual notification of FERPA rights which includes criteria for determining who constitutes a school official and what constitutes a legitimate educational interest.
- The definition of a school official may vary from one institution to another.

Question

Under FERPA, 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 other than what the institution includes in their agreement with the provider.

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 institution and as permitted by FERPA.

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 are often indirect identifying information in student data).

Properly de-identified metadata may be used by providers for other purposes (unless prohibited by their agreement with the institution).

FERPA is not the only game in town when it comes to student privacy

- Other Federal Laws
 - PPRA at the K-12 level
 - COPPA For children under 13
- State and Local Laws

COPPA

- 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
 - Administered by the Federal Trade Commission
 - See <http://www.business.ftc.gov/privacy-and-security/childrens-privacy> for more information

COPPA and Schools

- Can operators get consent from schools instead of parents to collect personal information from students?
 - Yes if for the use and benefit of the school and no other commercial purpose.
 - Teacher, school, district? Best practice is go through the institution.

FTC Act Enforcement

- Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.”
- Deception: a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances.
- Unfairness: practices that cause or are likely to cause substantial injury to consumers that are not outweighed by countervailing benefits to consumers or competition and are not reasonably avoidable by consumers.



What is 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* –
 1. Any protected information survey administered or distributed to a student by an local educational agency that is a recipient of funds under an applicable program (LEA) if the protected information survey is either not funded as part of a program administered by the Department or is funded as part of a program administered by the Department but to which a student is not required to submit;
 2. Any non-emergency, invasive physical examination or screening required by an LEA as a condition of attendance; administered by the school and scheduled by the school in advance; and, that is not necessary to protect the immediate health and safety of a student, with some exceptions; and
 3. Activities of an LEA involving collection, disclosure, or use of personal information collected from students for the purpose of marketing or sale (or to otherwise distribute such information to others for that purpose), with some exceptions.



Protection of Pupil Rights Amendment (PPRA)

- Amended in 2001 with No Child Left Behind Act
- Mostly known for its provisions dealing with surveys in K-12
- Includes limitations on using personal information collected from students for marketing
- May require parental notification and opportunity to opt out
- May require the development of policies in conjunction with parents
- Requires notification to parents and eligible students be provided regarding the conduct of school-sponsored surveys

Surveys – protected information

The following topics are considered **protected information** under the PPRA:

- Political affiliations or beliefs of the student or student's parent;
- Mental or psychological problems of the student or student's family;
- Sex behavior or attitudes;
- Illegal, anti-social, self-incriminating, or demeaning behavior;
- Critical appraisals of others with whom respondents have close family relationships;
- Legally recognized privileged relationships, such as with lawyers, doctors, or ministers;
- Religious practices, affiliations, or beliefs of the student or student's parent; or
- Income, other than as required by law to determine program eligibility.

Districts' responsibilities under PPRA

PPRA requires local educational agencies to develop and adopt policies, in consultation with parents, regarding:

- The right of parents to inspect, upon request, a survey created by a third party before the survey is administered or distributed by a school to students, and
- The procedure for granting a request by a parent for reasonable access to such survey within a reasonable period of time after the request is received.

Districts' responsibilities under PPRA (continued)

Under PPRA, the LEA must provide reasonable notice of the adoption or continued use of such policies directly to the parents of students enrolled in schools served by that agency.

At a minimum, the LEA must provide notice at least annually, at the beginning of the school year, and within a reasonable period of time after any substantive changes in such policies

Districts' responsibilities under PPRA (continued)

PPRA also requires LEAs:

- To adopt policies to protect student privacy in the event of the administration or distribution of any survey containing questions that ask students to reveal information from one of the eight PPRA-protected areas;
- To provide notification to parents, at least annually, at the beginning of the school year, of the specific or approximate dates during the school year when such a survey is scheduled or expected to be scheduled and an opportunity for parents to opt their students out of participation in any such survey.

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

Here’s a better question: Should individual teachers sign up for Free or “Freemium” services?



Using free or “freemium” educational services

Remember the FERPA’s requirements for institutions 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 institutions networks.



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

Question:

Should your staff be concerned if a TPP uses a “Click-Wrap” or Terms of Service agreement instead of a traditional contract?

Answer: It Depends

- Click-wrap or Terms of Service (TOS) agreements are not prohibited.
- Nothing in FERPA says that staff cannot click that "Accept" button.
- However, there are some considerations... (like everything else we've discussed today)

Click-Wrap Agreements

- These agreements are referred to as “click-wrap” agreements, and can operate as a provider’s legally-binding contract.
- Once a user at your institution clicks “I agree,” the terms of this agreement will likely govern what information the provider may collect from or about students and with whom they may share it.

Click-Wrap Agreements (cont'd)

- Click-Wrap agreements could potentially lead to a violation 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.
- The onus is on the institution to review the TOS to see if it is acceptable and complies with Federal and State law.
- The TPP has a click-wrap agreement to protect them, not necessarily you.



Privacy-Related TOS Provisions

- The example provisions are intended to give you a general idea of what to expect when reviewing a TOS.
 - Please keep in mind that specific language will vary from TOS to TOS.
 - Language matters and just because the TOS says that the vendor can do something does not mean that FERPA permits it.

Privacy-Related TOS Provisions

- The example provisions are intended to give you a general idea of what to expect when reviewing a TOS.
 - Please keep in mind that specific language will vary from TOS to TOS.
 - Language matters and just because the TOS says that the vendor can do something does not mean that FERPA permits it.



Challenge Reading!

An Application for the Connected Classroom

Found on the App Store

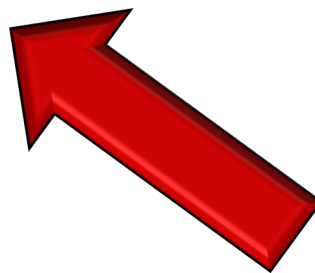
Website: https://www.cr_app.com



What is Data?

"The Challenge Reading! Application (hereafter referred to as 'CR App') considers data collected by the application to be all personally identifiable information (PII) and other non-public information that are directly related to the students in the system. Data include, but are not limited to, student data, and user content."

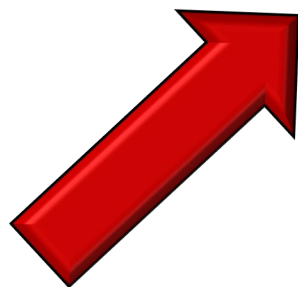
"The Challenge Reading! Application (hereafter referred to as 'CR App') considers data collected by the application to include only that information provided by the user in the course of using this service."



Data Collection

“CR App is not responsible for any data collected by third party services included on the CR App platform.”

“CR App will collect only that data necessary to fulfill the purposes specified in this agreement”



Common Thread Among the Data Provisions

- Narrow Focus
- Limited Scope
- Strong, simple definitions



Data De-Identification

- There is a significant amount of data available to providers of educational services.
 - Metadata on students' interaction with the service or app is often collected and analyzed to help improve the product and enable a provider to create more effective educational services.



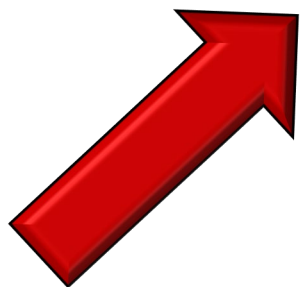
Data De-Identification (cont'd)

- Even stripped of identifiers, student data could still be identifiable (through demographic or contextual information collected by the app, or through information available elsewhere).

Rights and Licensing Provisions

"By using CR App, you grant CR App a non-exclusive, fully paid and royalty-free, worldwide, sublicensable, transferable, limited license to use, modify, delete, add to, reproduce in any media format through any media channels for any purpose any data or work submitted the app during the course of use."

"You agree to grant the provider (CR App), a limited, nonexclusive license solely for the purpose of performing its obligations as outlined in this Agreement. This agreement does not give provider any rights implied or otherwise, to data, content or intellectual property except as expressly stated in this agreement."



Rights and License to the Data

- Schools/Districts should maintain ownership of student data.
 - Some TOS include provisions that would grant providers an exclusive and irrevocable license to student data.
 - This can be a cause for concern.
 - If a license is granted, it should be limited and only allow student data to be used for educational purposes as outlined in the agreement.

Access

- FERPA requires schools and districts to make education records accessible to parents.
- To fulfill FERPA requirements, providers need to make student data available upon request.
- As a best practice, data should be passed from the provider to the school/district.

Data Use

“CR App will use data only for the purpose of fulfilling its duties and providing services under this agreement, and for improving services under this agreement.”

“CR App uses data to operate its website and deliver services. CR App may also use or transfer data to third parties to inform you of products and services available from CR App and its affiliates.



Data Use

“Data use” by a provider should be limited to the purposes outlined in the agreement with the school or district.

Always be on the lookout for any provision that contains the phrase “without providing notice to users”.

And remember, If the data is being disclosed under the School Officials Exception, look for the Legitimate Educational Interest!

Marketing and Advertising

- Information gathered in an online educational service or mobile application could be used to create a profile on a student.
- That profile could then be used to direct advertising/marketing materials to students.

Marketing and Advertising (cont'd)

- The language in a TOS should be clear that the data collected cannot be used to advertise or market to students.
 - Targeted advertising/marketing could violate privacy laws.

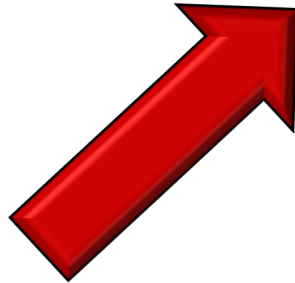


Security Controls

"You agree to not hold CR App responsible for any unauthorized data breaches."

"CR App stores and processes data in accordance with industry best practices. A summary of our security controls is described here:

https://www.cr_app.com/Security"



Security Controls

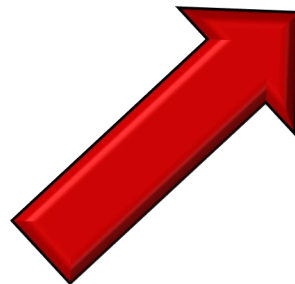


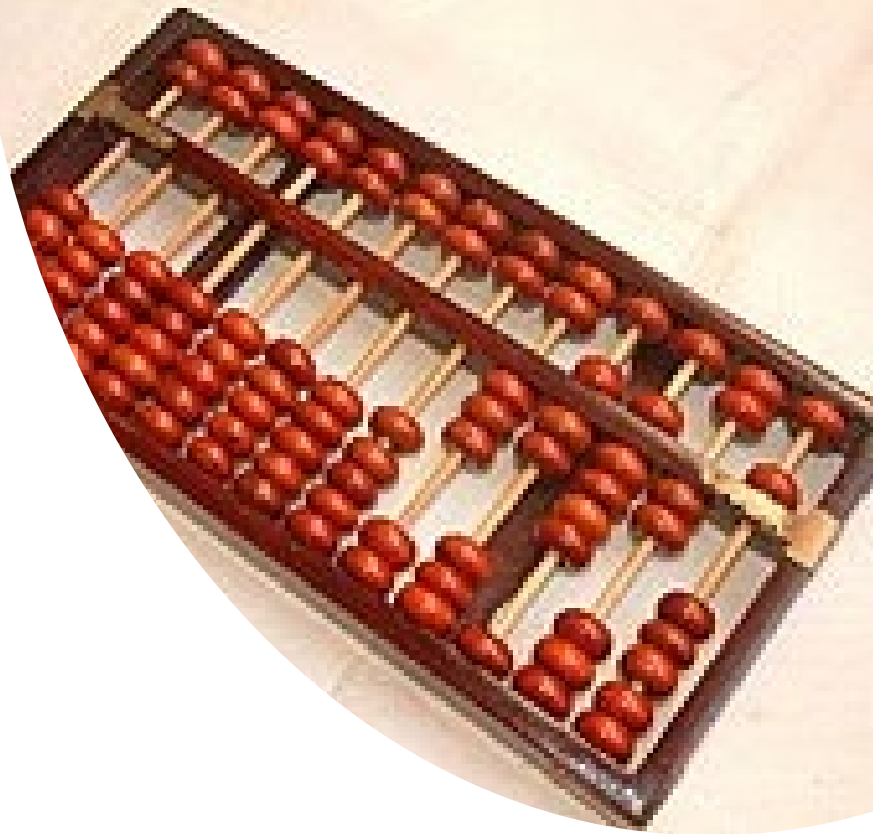
- Student data need to be protected, and a provider's TOS should include provisions outlining strong policies safeguarding those data.
- Failure to provide adequate security could lead to a FERPA violation.

Modification of the Terms of Service

"CR App may modify the terms of this agreement at any time. Notice of these changes will be available on our website. Please visit the website periodically to become aware of these changes."

"CR App will provide notice and obtain consent from the school prior to any change in the way data is collected used or shared under the terms of this agreement."





What Now?

“This session makes you not want to use any third party programs.”

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.

Don't be the "No" Person

- Educators want to use this technology.
- If they are told no, odds are they will do it anyways.
- By coming up with a policy and procedure you are able to ensure that the technology is used on your terms.

Developing District Policy

- Every school or district should have a policy in place for reviewing agreements before the service or application is used in the classroom.
 - Schools/Districts should establish a review process and/or have a designated individual review TOS before its adoption.
 - The service or application should be inventoried, evaluated, and support the school's and district's broader mission and goals.
- Get leadership buy-in and support for the new policy.



Policies and Procedures to Approve Educational Services

- Test and evaluate popular services to see if they are right for your district.
- Evaluate terms of service to ensure they are satisfactory.
- Consider developing a repository of “approved” apps.
- Training, Training, Training!

Protecting Student Privacy While Using Online Educational Services

- PTAC Training Video



~~Steal~~ Leverage the Work of your Peers

Many districts publish the list of apps that are acceptable in their districts

Other districts band together in consortiums to vet applications or negotiate TOS

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.



CONTACT INFORMATION

United States Department of Education,
Privacy Technical Assistance Center



(855) 249-3072
(202) 260-3887



privacyTA@ed.gov



<https://studentprivacy.ed.gov>



(855) 249-3073