



FEDERAL STUDENT PRIVACY UPDATE

FRANK MILLER

ACTING DIRECTOR

TRACY KOUMARÉ

EDUCATION PRIVACY POLICY ANALYST

STUDENT PRIVACY POLICY OFFICE
OFFICE OF PLANNING, EVALUATION,
AND POLICY DEVELOPMENT
U.S. DEPARTMENT OF EDUCATION

OFFICE REORGANIZATION

NEW NAME, CONSOLIDATED FUNCTIONS

- Effective January 2019, ED's student privacy functions were consolidated into the newly named **Student Privacy Policy Office (SPPO)**.
- The new office, reporting to the Assistant Secretary for Planning, Evaluation, and Policy Development, combines the functions previously provided by:
 - **Student Privacy Policy and Assistance Division**
 - Policy Development
 - Privacy Technical Assistance Center (PTAC)
 - **Family Policy Compliance Office (FPCO)**
 - Investigation and Enforcement of FERPA and PPRA violations



INSPECTOR GENERAL REPORT

Office of the Chief Privacy Officer's Processing of Family Educational Rights and Privacy Act Complaints

November 26, 2018

ED-OIG A09R0008

- “The Privacy Office did not have controls to ensure that it timely and effectively processed FERPA complaints...”
- “The Privacy Office had a longstanding and substantial backlog of unresolved FERPA complaints that prevented timely and effective resolution of new complaints it received.”
- “It also had a number of significant control weaknesses that hampered its ability to resolve FERPA complaints.”



REDUCING THE FERPA COMPLAINT BACKLOG

- By May 2018, there were 1,197 pending FERPA complaints.
- As of mid-April 2019, the backlog has been reduced by 51%, down to 591 open FERPA complaints, and continues to trend downward.
- SPPO has also begun providing all complainants with regular status updates on their complaints (at least every 120 days).



NEW INVESTIGATIONS PROCESSES

Improving the Effectiveness and Efficiency of FERPA Enforcement

December 20, 2018

“The Department is committed to protecting student privacy. To provide more timely and effective assistance to parents and students and to address a recommendation made by the Department’s Office of the Inspector General to “implement a risk-based approach to processing and resolving FERPA complaints,” the Department is modifying its investigatory practices to more efficiently address and resolve complaints and violations under FERPA.”

We now provide Resolution Assistance and Intermediation, in addition to formal complaint investigation.



TRANSPARENCY OF EDUCATION DATA PRACTICES

As part of the Department's [Strategic Plan for fiscal years 2018-2022](#), SPPO is conducting a review of LEA websites to assess how well the nation's school districts communicate with parents and students about their data practices.

Not an audit!

Reviewed LEAs will receive a technical assistance follow-up from PTAC, highlighting what they are doing well, and providing best practice recommendations.



SCHOOL SAFETY

Letter to School & College Legal Services of California

April 2018

Federal Commission on School Safety Report

December 2018

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

February 2019



FERPA RULEMAKING

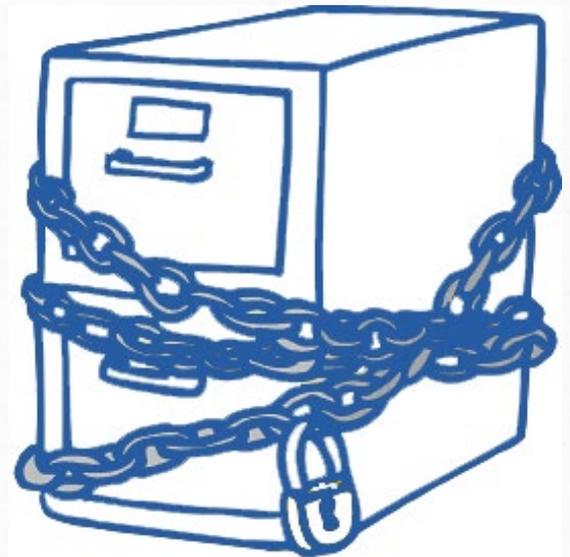
Coming Soon!



WHAT IS FERPA?

A federal privacy law that affords parents the right to:

- have **access** to their children's **education records**,
- seek to have the records **amended**, and
- **consent** to the **disclosure** of **personally identifiable information** from education records, **except** as provided by law.



THE THREE C'S OF FERPA

- In many ways, FERPA is not prescriptive. It is general in the ways it requires educational agencies to protect student information.
- It can be best summed up with 3 “C”s
 - FERPA is **Complex**
 - FERPA is **Conceptual**
 - FERPA is **Contextual**



WHAT RIGHTS DO PARENTS AND ELIGIBLE STUDENTS HAVE?

- Right to inspect and review education records;
- Right to request amendment of education records;
- Right to consent to disclosures, with certain exceptions; and
- Right to file a complaint with U.S. Department of Education regarding an alleged violation of FERPA.



USING EDUCATIONAL TECHNOLOGY IN THE CLASSROOM



WHAT IS AN ONLINE EDUCATIONAL SERVICE?

- 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.



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.
- How do schools protect student privacy in this new world of an “always connected” classroom?



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 district determines their own directory policy which includes an opt out provision.
- Some districts 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 teachers, 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, volunteers, 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 school or district 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 district to another.



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 school/district 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 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.*



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 school/district).



OBTAINING CONSENT ON BEHALF OF 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.



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 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.

Best Practice: establish district/school level policies governing use of free/freemium services, and to train teachers and staff accordingly.



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 school or district 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 school or district to review the TOS to see if it is acceptable and complies with Federal and State law.
- The service provider has a click-wrap agreement to protect themselves, not necessarily you.



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.



BEST PRACTICES FOR DATA DESTRUCTION

- Guidance was released March 2019 covers:
 - ✓ Gives an overview of the methods for data destruction
 - ✓ Discusses how methods relate to legal requirements
 - ✓ Establishes best practices for protecting PII

<https://studentprivacy.ed.gov/resources/best-practices-data-destruction>



DEFINING DESTRUCTION

- Data destruction is the process of removing information in a way that renders it unreadable (for paper records) or irretrievable (for digital records).



FERPA & DATA DESTRUCTION

WHAT ARE WE TALKING ABOUT?

- Not simply hitting “delete”
- Secure destruction so that it can’t be recovered
- Especially applicable to third-parties
- Not just Federal, but also State law in many cases



FERPA & DATA SECURITY

- **Clearing** – Removing data by software methods like overwriting the data or “formatting” the entire partition or disk
- **Purging** – Removing the data through physical or logical means such as applying strong magnetic fields to reduce the magnetic signature used to store data on disk
- **Destroying** – Removing the data by rendering the medium it is stored within unusable, typically through pulverizing, incinerating or shredding



FERPA & DATA DESTRUCTION

FERPA requires that PII from student records is protected from disclosure without consent unless it falls under one of the exceptions to FERPA.

Both the Studies and Audit or Evaluation exception to FERPA require written agreements which specify that the data must be destroyed when no longer needed!



FERPA & DATA DESTRUCTION

Best Practices for Written Agreements

- Bind individuals to the agreement
- Specify Points of Contact / Data Custodians
- **Set terms for data destruction**
- Maintain the right to audit
- Have plans to handle a data breach



WE'RE HERE TO HELP

SPPO's Privacy Technical Assistance Center (PTAC) is available to provide technical assistance and support.

PrivacyTA@ed.gov

<https://studentprivacy.ed.gov>



