

Responsibilities of Third-Party Service Providers under 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 <http://ptac.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

This document was developed by PTAC to assist online educational services providers, vendors, and contractors in understanding the Family Educational Rights and Privacy Act (FERPA). Our prior guidance, [Protecting Student Privacy While Using Online Educational Services](#), was intended for school audiences; this guidance presents the same material, but in a format geared toward third-party service providers.

It is important to remember that other Federal, state, tribal, or local laws may also protect the privacy of student information. This document will use the term “online educational services” to describe the broad category of tools and applications (apps) used by schools and districts, and the term “provider” to describe the third-party vendors, contractors, and other service providers that make these services available.

What is FERPA?

FERPA is a Federal law that protects personally identifiable information in students’ education records from unauthorized disclosure. It affords parents the right to access their child’s education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student (“eligible student”). The FERPA statute is found at [20 U.S.C. § 1232g](#), and the FERPA regulations are found at [34 CFR Part 99](#).

What are Education Records?

FERPA defines education records as “records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution” ([20 U.S.C. § 1232g \(a\)\(4\)\(A\)](#); [34 CFR § 99.3](#)). These records include, but are not limited to, transcripts, class lists, student course schedules, health records, student financial information, and student disciplinary records. It is important to note that any of these records maintained by a third party acting on behalf of a school or district are also considered education records.

What is Personally Identifiable Information?

FERPA defines the term personally identifiable information (PII) to include direct identifiers (such as a student's or other family member's name) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name). Indirect identifiers, metadata about students' interaction with an app or service, and even aggregate information can be considered PII under FERPA if a reasonable person in the school community could identify individual students based on the indirect identifiers together with other reasonably available information, including other public information.

How Are Providers Affected by FERPA?

Schools and districts often rely on providers to handle services they cannot efficiently provide themselves, such as

- student information systems;
- instructional improvement systems;
- online education programs or apps; or
- assessment systems.

Provider services are typically procured through a contract or formal written agreement.

School Official Exception

In some cases, providers need PII from students' education records in order to deliver the agreed-upon services. FERPA's school official exception to consent is most likely to apply to the schools' and districts' relationships with service providers. When schools and districts outsource institutional services or functions, FERPA permits the disclosure of PII from education records to contractors, consultants, volunteers, or other third parties *provided* that the outside party

1. performs an institutional service or function for which the agency or institution would otherwise use employees;
2. has been determined to meet the criteria set forth in the school's or district's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records;
3. is under the direct control of the agency or institution with respect to the use and maintenance of education records; and
4. uses education records only for authorized purposes and may not re-disclose PII from education records to other parties, unless the provider has specific authorization from the school or district to do so and it is otherwise permitted by FERPA. (See [34 CFR § 99.31\(a\)\(1\)\(i\)](#)).

When PII from education records is disclosed to the provider, FERPA still governs its use, and the school or district is responsible for its protection. PII from education records disclosed under FERPA's school official exception to consent may only be used for the purposes authorized by the respective school or district. In the relationship between the provider and the school or district, providers should remember that the school or district may require transparency about how student data obtained or collected under a contract or agreement are used, plans for data security and confidentiality of PII, and evidence that the school or district retains direct control with respect to the use and maintenance of PII at all times.

Directory Information Exception

Another exception to consent that permits the disclosure of PII from education records is the directory information exception. Information designated by the school or district as directory information may be disclosed without consent and used without restriction in conformity with the policy, unless the parent/guardian or eligible student opts out. Examples of directory information about students include name, address, telephone number, email address, date and place of birth, grade level, sports participation, and honors or awards received. Before a school or district can disclose directory information, it must first provide public notice to parents and eligible students of the types of information designated as directory information, the intended uses for the information, and the right of parents or eligible students to “opt out” of having their information shared.

Transparency about Data Use

As a best practice to promote transparency, both the provider and the school or district should post contracts or agreements on their public facing websites, including a list of data elements shared with the provider, and an explanation of how they are used and for what purpose. As a provider, you should only request or collect the minimum amount of PII that is needed to complete the assigned task.

You should be clear about your policies on data mining, including what data are being mined, and for what purpose. While data mining or scanning may sometimes be a necessary component of online services (e.g., for malware or spam detection or for personalization tools), mining or scanning for other purposes (e.g., targeted advertising directed to students or their parents) will likely violate federal or state privacy laws. Similarly, the collection, use, disclosure, or sale of PII to other parties for marketing purposes may also violate Federal or state law. Your use of PII from education records should be limited to only those purposes specified in the contract or agreement.

FERPA allows properly de-identified data to be used for other purposes, though providers planning to use de-identified student data should be clear about their methodologies for de-identification. If de-identified data will be transferred to another party, it is a best practice to contractually prohibit the transferee from attempting to re-identify any student data. Providers should also acknowledge whether anonymized metadata—a type of de-identified or partially de-identified data—will be used, and for what purposes.

Data Security and Confidentiality of PII

Providers should have a security plan with a system of checks and controls to ensure data security. Both providers and schools and districts should be clear on policies and procedures in the event of a data breach. Procedures for responding to a data breach should include when and how notification of the breach will be issued, and by whom. If a data breach occurs, it is best practice for the provider and the school or district to clearly state what has been breached, explain the measures taken to prevent future breaches, and describe the steps they will take to protect individuals affected by the breach. As a best practice, providers, schools, and districts may want to conduct periodic privacy audits to confirm that policies and procedures to ensure the security and confidentiality of the data are being followed.

You should also have a plan for data destruction once your contracted function is complete. The plan should include both a timeline and methodology for destroying the data. Providing certification of data destruction is a best practice.

School or District Control of PII

As a provider, you are required to be under the direct control of the school or district with regard to the use and maintenance of PII from education records if the disclosure was made under FERPA's school official exception. Agreements should prohibit PII from education records from being used for other purposes or re-disclosed without the school's or district's permission.

Changing the terms of service of a contract or agreement without notice or documentation makes it difficult for a school or district to demonstrate direct control of the maintenance and use of the PII. Therefore, schools or districts will be cautious about contracts that allow vendors to unilaterally modify provisions, and they will appreciate when you notify them of changes by clearly indicating the change, rather than burying it in a long document.

FERPA guarantees parents the right to access their child's education records, including those maintained by providers on behalf of the school or district, upon request within 45 days; some states provide a shorter window. As a best practice, parental access to their child's education records should be seamless, with providers giving the requested records to the school or district, who can confirm the parents' identity and provide them access to the records.

Maintaining the Trust of Parents

Parents will want to know what a provider is doing with their child's data. Transparency about what data are being collected and how they are being used is always the best policy for both schools and districts and their providers.

Additional Resources

The resources listed below provide additional best practice recommendations and guidance related to third-party responsibilities under FERPA. These and other privacy resources can be downloaded from the PTAC website, <http://ptac.ed.gov>.

- Privacy Technical Assistance Center, *Best Practices for Data Destruction* (2014): <http://ptac.ed.gov/document/best-practices-data-destruction>.
- Privacy Technical Assistance Center, *Checklist: Data Security* (2015): <http://ptac.ed.gov/content/checklist-data-security-dec-2011>.
- Privacy Technical Assistance Center, *Checklist: Data Sharing Agreement* (2015): <http://ptac.ed.gov/content/checklist-data-sharing-agreement-apr-2012>.
- Privacy Technical Assistance Center, *FERPA Exceptions Summary* (2014): <http://ptac.ed.gov/document/ferpa-exceptions-summary>.
- Privacy Technical Assistance Center, *Protecting Student Privacy While Using Online Educational Services* (2015): <http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services>.
- Privacy Technical Assistance Center, *Protecting Student Privacy While Using Online Educational Services: Model Terms of Service* (2015): <http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services-model-terms-service>.
- Privacy Technical Assistance Center, *Transparency Best Practices for Schools and Districts* (2014): <http://ptac.ed.gov/document/Transparency-Guidance>.