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 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

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 technologies raise questions about how best to protect student privacy during use. This document will address a number of these questions, and present some requirements and best practices to consider, when evaluating the use of online educational services.

What are Online Educational Services?

This document will address privacy and security considerations relating to computer software, mobile applications (apps), and web-based tools provided by a third-party to a school or district that students and/or their parents access via the Internet and use as part of a school activity. Examples include online services that students use to access class readings, to view their learning progression, to watch

video demonstrations, to comment on class activities, or to complete their homework. This document does not address online services or social media that students may use in their personal capacity outside of school, nor does it apply to online services that a school or district may use to which students and/or their parents do not have access (e.g., an online student information system used exclusively by teachers and staff for administrative purposes).

Many different terms are used to describe both the online services discussed in this document (e.g., Ed Tech, educational web services, information and communications technology, etc.) and the companies and other organizations providing these services. This document will use the term "online educational services" to describe this broad category of tools and applications, and the term "provider" to describe the third-party vendors, contractors, and other service providers that make these services available to schools and districts.

Is Student Information Used in Online Educational Services Protected by FERPA?

It depends. Because of the diversity and variety of online educational services, there is no universal answer to this question. The Family Educational Rights and Privacy Act (FERPA) (see 20 U.S.C. § 1232g and 34 CFR Part 99) protects personally identifiable information (PII) from students' education records from unauthorized disclosure. 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" (see 34 CFR § 99.3 definition of "education record"). FERPA also defines the term PII, which includes 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) (see 34 CFR § 99.3 definition of "personally identifiable information"). For more information about FERPA, please visit the Family Policy Compliance Office's Web site at http://www.ed.gov/fpco.

Some types of online educational services do use FERPA-protected information. For example, a district may decide to use an online system to allow students (and their parents) to log in and access class materials. In order to create student accounts, the district or school will likely need to give the provider the students' names and contact information from the students' education records, which are protected by FERPA. Conversely, other types of online educational services may not implicate FERPA-protected information. For example, a teacher may have students watch video tutorials or complete interactive exercises offered by a provider that does not require individual students to log in. In these cases, no PII from the students' education records would be disclosed to (or maintained by) the provider.

Online educational services increasingly collect a large amount of contextual or transactional data as part of their operations, often referred to as "metadata." Metadata refer to information that provides meaning and context to other data being collected; for example, information about how long a particular student took to perform an online task has more meaning if the user knows the date and time when the student completed the activity, how many attempts the student made, and how long the student's mouse hovered over an item (potentially indicating indecision).

Metadata that have been stripped of all direct and indirect identifiers are not considered protected information under FERPA because they are not PII. A provider that has been granted access to PII from education records under the school official exception may use any metadata that are not linked to FERPA-protected information for other purposes, unless otherwise prohibited by the terms of their agreement with the school or district.

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 (i.e., PII from education records) is implicated. If so, schools and districts must ensure that FERPA requirements are met (as well as the requirements of any other applicable federal, state, tribal, or local laws).

EXAMPLE 1: A district enters into an agreement to use an online tutoring and teaching program and discloses PII from education records needed to establish accounts for individual students using FERPA's school official exception. The provider sends reports on student progress to teachers on a weekly basis, summarizing how each student is progressing. The provider collects metadata about student activity, including time spent online, desktop vs. mobile access, success rates, and keystroke information. If the provider de-identifies these metadata by removing all direct and indirect identifying information about the individual students (including school and most geographic information), the provider can then use this information to develop new personalized learning products and services (unless the district's agreement with the provider precludes this use).

What Does FERPA Require if PII from Students' Education Records is Disclosed to a Provider?

It depends. Because of the diversity and variety of online educational services, there is no universal answer to this question. Subject to exceptions, the general rule under FERPA is that a school or district cannot disclose PII from education records to a provider unless the school or district has first obtained written consent from the parents (or from "eligible students," i.e., those who are 18 years of age or older or attending a postsecondary school). Accordingly, schools and districts must either obtain consent, or ensure that the arrangement with the provider meets one of FERPA's exceptions to the written consent requirement.

While disclosures of PII to create user accounts or to set up individual student profiles may be accomplished under the "directory information" exception, more frequently this type of disclosure will be made under FERPA's school official exception. "Directory information" is information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed (see 34 CFR § 99.3 definition of "directory information"). Typical examples of directory information include student name and address. To disclose student information under this exception, individual school districts must establish the specific elements or categories of directory information that they intend to disclose and publish those elements or categories in a public notice. While the directory information exception can seem to be an easy way to share PII from education

records with providers, this approach may be insufficient for several reasons. First, only information specifically identified as directory information in the school's or district's public notice may be disclosed under this exception. Furthermore, parents (and eligible students) generally have the right to "opt out" of disclosures under this exception, thereby precluding the sharing of information about those students with providers. Given the number of parents (and eligible students) who elect to opt out of directory information, schools and districts may not find this exception feasible for disclosing PII from education records to providers to create student accounts or profiles.

The FERPA school official exception is more likely to apply to schools' and districts' use of online educational services. Under the school official exception, schools and districts may disclose PII from students' education records to a provider as long as the provider:

1. Performs an institutional service or function for which the school or district would otherwise use its own employees;

2. Has been determined to meet the criteria set forth in 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 school or district with regard 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).

Two of these requirements are of particular importance. First, the provider of the service receiving the PII must have been determined to meet the criteria for being a school official with a "legitimate educational interest" as set forth in the school's or district's annual FERPA notification. Second, the framework under which the school or district uses the service must satisfy the "direct control" requirement by restricting the provider from using the PII for unauthorized purposes. While FERPA regulations do not require a written agreement for use in disclosures under the school official exception, in practice, schools and districts wishing to outsource services will usually be able to establish direct control through a contract signed by both the school or district and the provider. In some cases, the "Terms of Service" (TOS) agreed to by the school or district, prior to using the online educational services, may contain all of the necessary legal provisions governing access, use, and protection of the data, and thus may be sufficient to legally bind the provider to terms that are consistent with these direct control requirements.

When disclosing PII from education records to providers under the school official exception, schools and districts should be mindful of FERPA's provisions governing parents' (and eligible students') access to the students' education records. Whenever a provider maintains a student's education records, the

school and district must be able to provide the requesting parent (or eligible student) with access to those records. Schools and districts should ensure that their agreements with providers include provisions to allow for direct or indirect parental access. Under FERPA, a school must comply with a request from a parent or eligible student for access to education records within a reasonable period of time, but not more than 45 days after it has received the request. Some States have laws that require access to education records sooner than 45 days.

Schools and districts are encouraged to remember that FERPA represents a minimum set of requirements to follow. Thus, even when sharing PII from education records under an exception to FERPA's consent requirement, it is considered a best practice to adopt a comprehensive approach to protecting student privacy when using online educational services.

Do FERPA and the Protection of Pupil Rights Amendment (PPRA) Limit What Providers Can Do with the Student Information They Collect or Receive?

On occasion, providers may seek to use the student information they receive or collect through online educational services for other purposes than that for which they received the information, like marketing new products or services to the student, targeting individual students with directed advertisements, or selling the information to a third party. If the school or district has shared information under FERPA's school official exception, however, the provider cannot use the FERPA-protected information for any other purpose than the purpose for which it was disclosed.

Any PII from students' education records that the provider receives under FERPA's school official exception may only be used for the specific purpose for which it was disclosed (i.e., to perform the outsourced institutional service or function, and the school or district must have direct control over the use and maintenance of the PII by the provider receiving the PII). Further, under FERPA's school official exception, the provider may not share (or sell) FERPA-protected information, or re-use it for any other purposes, except as directed by the school or district and as permitted by FERPA.

It is important to remember, however, that student information that has been properly de-identified or that is shared under the "directory information" exception, is not protected by FERPA, and thus is not subject to FERPA's use and re-disclosure limitations.

EXAMPLE 2: A district contracts with a provider to manage its cafeteria account services. Using the school official exception, the district gives the provider student names and other information from school records (not just directory information). The provider sets up an online system that allows the school, parents, and students to access cafeteria information to verify account balances and review the students' meal selections. The provider cannot sell the student roster to a third party, nor can it use PII from education records to target students for advertisements for foods that they often purchase at school under FERPA because the provider would then be using FERPA-protected information for different purposes than those for which the information was shared.

FERPA is not the only statute that limits what providers can do with student information. The Protection of Pupil Rights Amendment (PPRA) provides parents with certain rights with regard to some marketing activities in schools. Specifically, PPRA requires that a school district must, with exceptions, directly notify parents of students who are scheduled to participate in activities involving the collection, disclosure, or use of personal information collected from students for marketing purposes, or to sell or otherwise provide that information to others for marketing purposes, and to give parents the opportunity to opt-out of these activities. 20 U.S.C. § 1232h(c)(2)(C)(i). Subject to the same exceptions, PPRA also requires districts to develop and adopt policies, in consultation with parents, about these activities. 20 U.S.C. § 1232h(c)(1)(E) and (c)(4)(A). PPRA has an important exception, however, as neither parental notice and the opportunity to opt-out nor the development and adoption of policies are required for school districts to use students' personal information that they collect from students for the exclusive purpose of developing, evaluating, or providing educational products or services for students or schools. 20 U.S.C. § 1232h(c)(4)(A).

While FERPA protects PII from education records maintained by a school or district, PPRA is invoked when personal information is collected from the student. The use of online educational services may give rise to situations where the school or district provides FERPA-protected data to open accounts for students, and subsequent information gathered through the student's interaction with the online educational service may implicate PPRA. Student information collected or maintained as part of an online educational service may be protected under FERPA, under PPRA, under both statutes, or not protected by either. Which statute applies depends on the content of the information, how it is collected or disclosed, and the purposes for which it is used.

It is important to remember that even though PPRA only applies to K-12 institutions, there is no time-limit on the limitations governing the use of personal information collected from students for marketing purposes. So, for example, while PPRA would not limit the use of information collected from college students for marketing, it would restrict the use of information collected from students while they were still in high school (if no notice or opportunity to opt-out was provided) even after those students graduate.

EXAMPLE 3: A district contracts with an online tutoring service using the school official exception. As part of the service, the provider uses data about individual students to personalize learning modules for the district's students. This does not implicate the PPRA because the activity falls under the PPRA exception for educational services and products. This use of data about individual students is similarly permissible under FERPA because the provider is only using any FERPA-protected information for the purposes for which it was shared.

EXAMPLE 4: A district contracts under the school official exception with a provider for basic productivity applications to help educate students: email, calendaring, web-search, and document collaboration software. The district sets up the user accounts, using basic enrollment information (name, grade, etc.) from student records. Under FERPA, the provider may not use data about individual student preferences gleaned from scanning student content to target ads to individual students for clothing or toys, because using the data for these purposes was not authorized by the district and does not constitute a legitimate educational interest as specified in the district's annual notification of FERPA rights.

PPRA would similarly prohibit targeted ads for clothing or toys, unless the district had a policy addressing this and parents were notified and given the opportunity to opt-out of such marketing. In spite of these limitations, however, the provider may use data (even in individually identifiable form) to improve its delivery of these applications, including spam filtering and usage monitoring. The provider may also use any non-PII data, such as metadata with all direct and indirect identifiers removed, to create new products and services that the provider could market to schools and districts.

Schools and districts should be aware that neither FERPA nor the PPRA absolutely prohibits them from allowing providers to serve generalized, non-targeted advertisements. FERPA would not prohibit, for example, a school from selling space on billboards on the football field, nor would it prohibit a school or district from allowing a provider acting as a school official from serving ads to all students in email or other online services.

Finally, schools and districts should remember their important role in setting policies to protect student privacy. While FERPA and PPRA provide important protections for student information, additional use or disclosure restrictions may be advisable depending on the situation and the sensitivity of the information. Any additional protections that a school or district would like to require should be documented in the written agreement (the contract or TOS) with the provider.

What are Some Other Best Practices for Protecting Student Privacy When Using Online Educational Services?

Regardless of whether FERPA or PPRA applies to a school's or district's proposed use of online educational services, the Department recommends that schools and districts follow privacy, security, and transparency best practices, such as:

- **Maintain awareness of other relevant federal, state, tribal, or local laws.**

  FERPA and PPRA are not the only laws that protect student information. Other federal, state, tribal, or local laws may apply to online educational services, and may limit the information that can be shared with providers. In particular, schools and districts should be aware of and

consider the requirements of the Children's Online Privacy and Protection Act (COPPA) before using online educational services for children under age 13. In general, COPPA applies to commercial Web sites and online services directed to children and those Web sites and services with actual knowledge that they have collected personal information from children. Absent an exception, these sites must obtain verifiable parental consent prior to collecting personal information from children. The Federal Trade Commission (FTC) has interpreted COPPA to allow schools to exercise consent on behalf of parents in certain, limited circumstances (see http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#Schools).

- **Be aware of which online educational services are currently being used in your district.**

  Conduct an inventory of the online educational services currently being used within your school or district. Not only will this help assess the scope and range of student information being shared with providers, but having a master list of online educational services will help school officials to collaboratively evaluate which services are most effective, and help foster informed communication with parents.

- **Have policies and procedures to evaluate and approve proposed online educational services**.

  Establish and enforce school and district-wide policies for evaluating and approving online educational services prior to implementation. Schools and districts should be clear with both teachers and administrators about how proposed online educational services can be approved, and who has the authority to enter into agreements with providers. This is true not only for formal contracts, but also for consumer-oriented "Click-Wrap" software that is acquired simply by clicking "accept" to the provider's TOS. With Click-Wrap agreements, the act of clicking a button to accept the TOS serves to enter the provider and the end-user (in this case, the school or district) into a contractual relationship akin to signing a contract.

  Most schools or districts already have processes in place for evaluating vendor contracts for privacy and security considerations; using these established procedures may be the most effective way to evaluate proposed online educational services. It is particularly important that teachers and staff not bypass internal controls in the acquisition process when deciding to use free online educational services. To ensure that privacy and security concerns relating to these free services are adequately considered, the Department recommends that free online educational services go through the same (or a similar) approval process as paid educational services to ensure that they do not present a risk to the privacy or security of students' data or to the schools and district's IT systems. Following standard internal controls, including testing, will also enable the schools and district's IT personnel to assist in the implementation process. Simple and more streamlined processes will, of course, generate greater compliance.

- **When possible, use a written contract or legal agreement.**

  As mentioned above, the use of online educational services usually involves some form of a

contract or legal agreement between the school and the provider. Having a written contract or legal agreement helps schools and districts maintain the required "direct control" over the use and maintenance of student data. Even when FERPA is not implicated, the Department recommends using written agreements as a best practice. When drafting and reviewing these contracts, the Department recommends the inclusion of certain provisions:

- Security and Data Stewardship Provisions. Make clear whether the data collected belongs to the school/district or the provider, describe each party's responsibilities in the event of a data breach (see PTAC's Data Breach Response Checklist), and, when appropriate, establish minimum security controls that must be met and allow for a security audit.

- Collection Provisions. Be specific about the information the provider will collect (e.g., forms, logs, cookies, tracking pixels, etc.).

- Data Use, Retention, Disclosure, and Destruction Provisions. Define the specific purposes for which the provider may use student information, and bind the provider to only those approved uses. If student information is being shared under the school official exception to consent in FERPA, then it would also be a best practice to specify in the agreement how the school or district will be exercising "direct control" over the third party provider's use and maintenance of the data. Specify with whom the provider may share (re-disclose) student information, and if PII from students' education records is involved, ensure that these provisions are consistent with FERPA. Include data archival and destruction requirements to ensure student information is no longer residing on the provider's systems after the contract period is complete. When appropriate, define what disclosure avoidance procedures must be performed to de-identify student information before the provider may retain it, share it with other parties, or use it for other purposes.

- Data Access Provisions. Specify whether the school, district and/or parents (or eligible students) will be permitted to access the data (and if so, to which data) and explain the process for obtaining access. This is especially important if the online educational services will be creating new education records that will be maintained by the provider on behalf of the school or district, as FERPA's requirements regarding parental (or eligible students') access will then apply. To avoid the challenges involved in proper authentication of students' parents by the provider, the Department recommends that the school or district serve as the intermediary for these requests, wherein the parent requests access to any education records created and maintained by the provider directly from the school or district, and the school or district then obtains the records from the provider to give back to the parent.

- Modification, Duration, and Termination Provisions. Establish how long the agreement will be in force, what the procedures will be for modifying the terms of the agreement

(mutual consent to any changes is a best practice), and what both parties' responsibilities will be upon termination of the agreement, particularly regarding disposition of student information maintained by the provider.

- Indemnification and Warranty Provisions. Carefully assess the need for and legality of any such provisions and determine whether applicable state or tribal law prohibits or limits the school's or district's ability to indemnify a provider. Analyze whether there should be indemnification provisions in which the provider agrees to indemnify the school or district, particularly relating to a school's or district's potential liabilities resulting from a provider's failure to comply with applicable federal, state, or tribal laws. Given that the Department looks to schools and districts to comply with FERPA and PPRA, be specific about what you will require the provider to do in order to comply with applicable state and federal laws, such as FERPA and PPRA, and what the provider agrees to do to remedy a violation of these requirements and compensate the school or district for damages resulting from the provider's violation.

- **Extra steps are necessary when accepting Click-Wrap licenses for consumer apps.**

  Schools and districts sometimes can't negotiate agreements with providers of consumer apps, and are faced with a choice to accept the providers' TOS or not use the app. Extra caution and extra steps are warranted before employing Click-Wrap consumer apps:

  - Check Amendment Provisions. In addition to reviewing for the above terms, you should review the TOS to determine if the provider has retained the right to amend the TOS without notice. If the provider will be using FERPA-protected information, schools and districts should exercise caution when entering into Click-Wrap agreements that allow for amendment without notice, given FERPA's requirement to maintain "direct control" over the use and maintenance of the information under the school official exception. It is a best practice to review these agreements regularly to determine if any provisions have changed, and if so, to re-evaluate whether to continue using the service.

  - Print or Save the TOS. When accepting a Click-Wrap agreement, you should save a copy of the TOS that you have agreed to. You can either download and save a digital copy, or print and file a copy.

  - Limit Authority to Accept TOS. One potential issue with Click-Wrap agreements is that they can be easily accepted, without going through normal district or school approval channels. Individual teachers may not understand the specifics of how the provider will use and secure student data. Districts or schools should develop policies outlining when individual teachers may download and use Click-Wrap software.

EXAMPLE 5: A teacher who has many remote students wants to foster increased collaboration and socialization among her students. Pursuant to her district's policy, she selects a service from a district-approved list of providers, and accepts the provider's Click-Wrap agreement before creating the user accounts for all students (including those who opted out of directory information). Her students successfully participate in a students-only social collaboration space.

EXAMPLE 6: A teacher wants students to be able to share photographs and videos online and identifies an app that will allow this sharing. He creates user accounts for all students (including those who opted out of directory information) and accepts the app's Click-Wrap agreement without reading it. The TOS allow the provider to use the information for a variety of non-educational purposes, including selling merchandise. The district discovers that this service is being used and determines that the TOS violate FERPA. The district proceeds to block access to the service from district computers, and begins negotiations with the provider to delete the user accounts and any information attached to them.

- **Be transparent with parents and students.**

  The Department encourages schools and districts to be as transparent as possible with parents and students about how the school or district collects, shares, protects, and uses student data. FERPA requires that schools and districts issue an annual notification to parents and eligible students explaining their rights under FERPA (34 CFR § 99.7), and many schools and districts elect to combine their directory information policy public notice, required pursuant to §99.37 of the regulations, with their annual notice of rights. PPRA also requires schools and districts to provide parents and students with effective notice of their PPRA rights, to provide notice to parents of district policies (developed and adopted in consultation with parents) regarding specific activities, and to notify them of the dates of specific events and the opportunity to opt out of participating in those events. Beyond FERPA and PPRA compliance, however, the Department recommends that schools and districts clearly explain on their Web sites how and with whom they share student data, and that they post any school and district policies on outsourcing of school functions, including online educational services. Schools and districts may also want to post copies of the privacy and security provisions of important third party contracts.

  With online educational services, it can often be unclear what information is being collected while students are using the technology. Even when this information is not protected by FERPA or other privacy laws, it is a best practice to inform students and their parents of what information is being collected and how it will be used. When appropriate, the Department recommends that schools or districts develop an education technology plan that addresses student privacy and information security issues, and solicit feedback from parents about the plan prior to its implementation or the adoption of new online education services.

Transparency provides parents, students, and the general public with important information about how the school or district protects the privacy of student data. Greater transparency enables parents, students, and the public to develop informed opinions about the benefits and risks of using education technology and helps alleviate confusion and misunderstandings about what data will be shared and how they will be used.

- **Consider that parental consent may be appropriate.**

  Even in instances where FERPA does not require parental consent, schools and districts should consider whether consent is appropriate. These are individual determinations that should be made on a case-by-case basis.

Additional Resources

Materials below include links to resources that provide additional best practice recommendations and guidance relating to use of online educational services. Please note that these resources do not necessarily address the particular legal requirements, including FERPA, that your school and district need to meet when collecting, storing, disseminating, or releasing education records to a provider. It is always a best practice to consult legal counsel to determine the applicable federal, state, tribal, and local requirements prior to entering into contractual agreements with providers. Some resources prepared by third-party experts are included as well.

- Family Policy Compliance Office, U.S. Department of Education, *Model Notice for Directory Information:* *http://www.ed.gov/policy/gen/guid/fpco/ferpa/mndirectoryinfo.html*
- National Institute of Standards and Technology, Computer Security Resource Center: http://csrc.nist.gov/publications/
- National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing* (2011): http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
- National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publications (FIPS) 199* (2004): http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- Privacy Technical Assistance Center, U.S. Department of Education: http://ptac.ed.gov
- Privacy Technical Assistance Center, U.S. Department of Education, *Checklist – Data Breach Response* (2012): http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf
- Privacy Technical Assistance Center, U.S. Department of Education, *Written Agreement Checklist* (2012): http://ptac.ed.gov/sites/default/files/data-sharing-agreement-checklist.pdf
- U.S. Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions - COPPA AND SCHOOLS* (2013): http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#Schools
- U.S. Federal Trade Commission, *FTC Strengthens Kid's Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Protection Rule* (2012): http://www.ftc.gov/opa/2012/12/coppa.shtm

Glossary

Directory Information is information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Typically, "directory information" includes information such as name, address, telephone listing, date and place of birth, participation in officially recognized activities and sports, and dates of attendance. A school may disclose "directory information" to third parties without consent if it has given public notice of the types of information which it has designated as "directory information," the parent's or eligible student's right to restrict the disclosure of such information, and the period of time within which a parent or eligible student has to notify the school in writing that he or she does not want any or all of those types of information designated as "directory information." 34 CFR § 99.3 and 34 CFR § 99.37.

Education records means records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations. 34 CFR § 99.3.

Eligible Student means a student to whom FERPA rights have transferred upon turning 18 years of age, or upon enrolling in a post-secondary institution at any age. 34 CFR § 99.3.

Personally identifiable information (PII) is a FERPA term referring to identifiable information that is maintained in education records and includes direct identifiers, such as a student's name or identification number, indirect identifiers, such as a student's date of birth, or other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR § 99.3, for a complete definition of PII specific to education records and for examples of other data elements that are defined to constitute PII.

Personal Information Collected from Students is a PPRA term referring to individually identifiable information including a student or parent's first and last name; a home or other physical address (including street name and the name of the city or town); a telephone number; or a Social Security identification number collected from any elementary or secondary school student. 20 U.S.C. § 1232h(c)(6)(E).

School Official means any employee, including teacher, that the school or district has determined to have a "legitimate educational interest" in the personally identifiable information from an education record of a student. School officials may also include third party contractors, consultants, volunteers, service providers, or other party with whom the school or district has outsourced institutional services or functions for which the school or district would otherwise use employees under the school official exception in FERPA. 34 CFR § 99.31(a)(1).