

The Family Educational Rights and Privacy Act: 7 Myths — and the Truth

By STEVEN J. MCDONALD

An extraordinary amount of the national discussion since the shootings at Virginia Tech a year ago has focused on the role that the Family Educational Rights and Privacy Act, or Ferpa, the federal statute governing the privacy of student records, played in that tragedy. What that discussion has revealed most notably is that, although colleges have been subject to Ferpa for more than 30 years, and although few if any statutes have such wide-reaching, everyday application on our campuses, most of us still don't know much about it. In a way, Ferpa is the Rodney Dangerfield of statutes: While there is a great deal to it, it just doesn't get much respect.

In an effort to bring about greater clarity, the Family Policy Compliance Office, the office within the Education Department that oversees and enforces Ferpa, recently proposed the first major amendments to the regulations since 2000. For the most part, those amendments would simply codify and reinforce existing guidance. In a few circumstances, they would actually expand our already considerable discretion to disclose student records and information. But even those amendments will do no good unless we begin to pay attention to Ferpa and dispel a number of all-too-common myths about it that continue to get in the way of our doing the right thing for our students. Those myths include:

1. Ferpa applies to all information about our students. In fact, Ferpa governs the disclosure only of "records" and information from "records," not information generally. Personal knowledge is not subject to Ferpa, and its disclosure is therefore not prohibited by Ferpa — even if it also happens to be recorded.

Thus, for example, a professor who observes a student behaving oddly in a classroom, a resident assistant who notices a disturbing change in a student's temperament, or an adviser who sees a student become increasingly withdrawn and uncommunicative is free, as far as Ferpa is concerned, to raise the concern with others — and should do so. We do neither the student nor ourselves a favor if we don't try to reach out and deal with such situations when we still have the opportunity.

Ordinarily, if circumstances allow, it is preferable to raise such concerns first with those trained to evaluate and deal with them, such as campus mental-health professionals, campus police, or appropriate student-affairs officials. When the situation appears to be urgent, however, it is both appropriate and permissible to disclose the concern as broadly as seems necessary.

2. Ferpa makes it virtually impossible to disclose anything to anyone. The statute does apply broadly to almost all recorded student information in our possession, but, even so, it still offers us considerable leeway.

First, it exempts entirely from its coverage several categories of records, including, most significantly, "law-enforcement records." Records that are created by a campus's law-enforcement unit — be it commissioned police or noncommissioned security — at least in part for law-enforcement purposes and that are maintained by that unit may, under Ferpa, be freely shared with anyone for any reason. It makes no difference whether the creation of those records was also motivated by internal disciplinary or other reasons or whether they are shared with others on the campus for their own use. The copies of any such records that are shared with other offices do become subject to Ferpa, but the originals in the law-enforcement unit's possession remain entirely free of Ferpa's restrictions.

In addition, Ferpa offers no fewer than 15 exceptions to its general prohibition on the disclosure of student records and the information they contain (see list on following page), and a 16th exception has been proposed.

Finally, Ferpa also allows us to disclose records that have been thoroughly "anonymized," or scrubbed of personally identifiable information, and we are always free to disclose any student record with the student's consent.

At the same time, Ferpa also never compels us to use any of that leeway. Rather, it gives us discretion to do so under the specified circumstances if we deem it appropriate — and therefore requires us to make a decision, a situation that can lead to paralysis. But if we choose not to disclose student information when we would be permitted to do so, whether for legitimate policy reasons or by default, we should not use Ferpa as an excuse and thereby perpetuate this unfortunate and potentially harmful myth.

3. Ferpa prohibits us from sharing any student information with parents unless students specifically consent. As useful as such a "rule" might be in this age of attack-helicopter parents, and while we are free to adopt it as a policy matter if we so wish, we are not compelled to do so by the statute. Primary control over a student's records does shift from the parents to the student when the student enrolls in college, even if the student is still a minor, but primary control is not the same as total control. Institutions can disclose student information to parents under any number of circumstances.

Among the circumstances:

- If either parent claims the student as a federal tax dependent, the institution may, with confirmation of that status, disclose any and all information it has about the student to both parents, regardless of the student's age or whether there is an emergency.
- If the student is under 21, the institution may inform the student's parents of any violations of its alcohol or drug policies, regardless of whether the student is a tax dependent or whether there is an emergency.
- If the institution reasonably believes that there is a health or safety emergency involving the student, the institution may alert the student's parents and seek their

assistance, regardless of the student's age or whether the student is a tax dependent.

Moreover, we can make such disclosures even if the student has asked us not to. Ferpa doesn't give students a veto over any of the permitted disclosures except the one for "directory information."

4. We can't rely on the "health or safety emergency" exception if there's any uncertainty at all about whether we're facing imminent catastrophe. The many reviews and reports after Virginia Tech found the greatest confusion about, and resulting fear of, the Ferpa exception for disclosures to "appropriate persons" in connection with an "emergency" involving the "health or safety of the student or other persons." Much of that confusion and fear, it seems, can be traced to the regulation's statement that each of those terms must be "strictly construed." Additional guidance, intended to head off backlash against foreign students after September 11, 2001, indicates that the "danger" used to justify invocation of the exception must be both "serious" and "imminent."

To be sure, Ferpa is a privacy statute, and we certainly must acknowledge our students' legitimate interest in maintaining their privacy, but Ferpa does not make that interest an absolute, unassailable priority. Nor does Ferpa require that the situation at hand be a "red level" crisis, that only the intended disclosure will avert it, and that we be absolutely sure of both those conditions before proceeding.

Rather, Ferpa recognizes that decisions about when emergency disclosure is needed and what disclosure is appropriate must often be made in the heat of the moment, before all of the facts are, or could possibly be, known. In other guidance, the Family Policy Compliance Office has expressly stated that it will not fault good-faith decisions in that regard even if they turn out, in hindsight, to have been wrong: "This office will not substitute its judgment for what constitutes a true threat or emergency unless the determination appears manifestly unreasonable or irrational."

The reality, then, is that there is little to worry about when relying on the health-or-safety-emergency exception. But to make that point even clearer, the compliance office has just proposed to amend the regulation by eliminating the "strictly construed" provision and replacing it with a codification of its previous guidance. Those changes, the compliance office states, are intended to underscore that colleges have far "greater flexibility and deference" than we may have realized to "bring appropriate resources to bear on a circumstance that threatens the health or safety of individuals." We should not hesitate to take advantage of that flexibility and deference when it reasonably appears to be in the best interest of our students and institution that we do so.

5. Both Ferpa and Hipaa, the Health Insurance Portability and Accountability Act, prohibit the disclosure of student medical records to anyone. Ferpa's handling of student medical records and its "Alphonse and Gaston" interplay with Hipaa are, without question, counterintuitive and difficult to understand at first look. To begin, Hipaa expressly excludes from the coverage of its privacy provisions any records that are

subject to Ferpa. Ferpa in turn provides that "treatment records" — records created by medical professionals in the course of treating a student — are not subject to Ferpa. Back to Hipaa, which nevertheless excludes "treatment records" as well.

But there's a hitch: Such records are exempt from Ferpa's restrictions only as long as they are not shared with anyone other than those involved in providing the treatment. To the extent they are shared with anyone else, they are subject to the same disclosure restrictions under Ferpa as any other student records. (Other medically related student records that do not involve "treatment," such as disability-accommodation records or immunization verifications, are always subject to Ferpa and its general restrictions, and not to Hipaa.)

The reason for that convoluted, backhanded definition is not that Congress wanted student medical records to go wholly unprotected, but, rather, that it didn't want them to be subject to students' near-absolute right under Ferpa to "inspect and review" their own records. As long as such records remain in this Ferpa-Hipaa limbo, they are subject instead only to the typically more-limited state rules concerning when patients may access their own medical records.

The net result is that medically related student records — whether "treatment" records or not — are never subject to Hipaa's privacy provisions, are always (really) subject to Ferpa, and are, for all practical purposes, treated no differently under Ferpa than any other student records.

Campus medical professionals continue to be bound as well by whatever limits are imposed upon them by applicable state medical-confidentiality laws, but even those laws generally allow consultation with other medical professionals involved in treating the student, whether on or off the campus, and appropriate disclosures when deemed necessary to avert a serious threat to the health or safety of the student or others. Moreover, others on the campus who may have access to medically related student records generally are not subject to such state laws. They remain free to disclose those records to other college officials with a job-related need to know, in response to a health or safety emergency, to parents of a dependent student, in compliance with a subpoena, or in any of the other ways that Ferpa allows student records to be disclosed.

6. The consequences of violating Ferpa are devastating, so the safest course is to disclose nothing. It is true that withholding student information is, almost always, "safe," at least as far as Ferpa is concerned. At the college level, the only person who ever has a legally enforceable right under Ferpa to know what is in a student's records is the student. All of the exceptions that permit broader disclosure are entirely discretionary, so there is no legal consequence under Ferpa in choosing not to disclose.

Disclosing student-record information is, however, almost equally safe as far as Ferpa is concerned. In the 2002 case *Gonzaga University v. Doe*, the U.S. Supreme Court held that there is no private right of action under Ferpa. As a result, we cannot be sued by

aggrieved students or others even if we stray over the line of permissible disclosure. Their only recourse is to file a complaint with the Family Policy Compliance Office.

Moreover, while the enforcement tools in that office's arsenal are theoretically severe — potentially including the termination of federal support — Ferpa imposes no penalty whatever for making a single, honest mistake. Rather, it reserves its consequences only for institutions that have a "policy or practice" of violating its provisions. Even then sanctions may be imposed "only if . . . compliance cannot be secured by voluntary means" — in other words, only if an institution engages in repeated, intentional violations. In the 34 years since Ferpa's enactment, the compliance office has reviewed hundreds of complaints, and has found numerous violations, but has never once terminated even a single penny of federal money.

Nevertheless, Ferpa's "nuclear option" is frequently cited to limit or deny disclosure of student information, usually out of unwarranted fear of liability — and occasionally in an effort to cut off an opponent's policy argument in favor of disclosure. Instead of fretting about that extraordinarily remote threat, we should focus our discussions and decisions about disclosure on what is best for our students, secure in the knowledge that Ferpa gives us considerable room to do so.

7. Ferpa is seriously broken and needs to be fixed. That is perhaps the biggest myth of all. There is no question that Ferpa can be frustrating and even paralyzing. Its numerous provisions can be confusing, simply by virtue of their sheer quantity. They occasionally seem to point to conflicting conclusions. All too often they appear to be nothing more than micromanaging.

And yet Ferpa is actually quite flexible and forgiving. Only rarely does it restrict us from communicating about our students when we need to do so, and hardly ever does it compel communication about our students. It gives us considerable discretion to do what we, in our best judgment, think should be done. The consequences Ferpa imposes for good-faith mistakes are, in reality, little more than a gentle admonishment to learn from those mistakes and do better next time.

The real problem with Ferpa is that its flexibility is not well or widely understood. But if that is the problem, making Ferpa even more complex, by grafting ever-more-detailed exceptions — and exceptions to exceptions — onto it, is unlikely to help. While no doubt well intentioned, the many calls and proposals for major substantive revisions to Ferpa in the aftermath of Virginia Tech would, if adopted, probably yield only more confusion — and more paralysis — rather than clarity and better decision making.

Instead of trying to "fix" Ferpa, we should give it the respect it is due by learning what it actually provides, rather than relying on the myths we've heard about it. There is nothing to fear in Ferpa itself.

Steven J. McDonald is general counsel at the Rhode Island School of Design.

KEY EXCEPTIONS TO FERPA

- Under the Family Educational Rights and Privacy Act, which governs the disclosure of student records, colleges may disclose any and all student records and information to faculty and staff members, to lawyers, accountants, and other outside contractors retained to provide services to the institution or to perform functions on its behalf, and even to other students who are acting on the institution's behalf — such as student representatives on a disciplinary committee — as long as they reasonably need access to the records and information to do their jobs. To use that exception, colleges must notify their students at least annually of how broadly they intend to employ it.
- Colleges may disclose any and all such records and information to officials at other colleges at which a student seeks or intends to enroll or is simultaneously enrolled. (Again, colleges must notify their students at least annually of their practice of doing so.)
- Unless a student has affirmatively opted out, colleges may disclose to anyone a fairly long list of "directory information," including name; physical and e-mail addresses; telephone numbers; major; degrees, honors, and awards received; participation in officially recognized activities and sports; photographs; and more. They cannot, however, disclose such information in a way that implicitly discloses nondirectory information as well. For example, colleges cannot disclose a list of "just names and addresses" in response to an inquiry about students who achieved a specified grade-point average, who took a particular course, or who were brought before a disciplinary committee in a given year. Doing so would reveal more about those students than "just" their names and addresses.
- If a college determines through its disciplinary system that a student committed certain serious offenses involving actual or threatened violence, it may disclose to anyone the student's name, the violation that occurred, and the sanction that was imposed.
- Colleges may disclose any such records or information in response to a subpoena from a court or agency having jurisdiction over them, although they generally must notify the student first.
- Colleges may disclose student records and information to students' parents in certain circumstances.
- Colleges may disclose such records and information to "appropriate parties" in connection with a "health or safety emergency."

Originally appeared in the *Chronicle of Higher Education*
Section: Commentary
Volume 54, Issue 32, Page A53
April 18, 2008

VIA E-MAIL AND U.S. MAIL

To: Students Involved in XYZ Disciplinary Hearing

Re: State of Rhode Island v. XYZ

As you may know, XYZ, a former student at RISD, is currently facing criminal charges in connection with an incident on campus this past spring semester. As part of the “discovery” phase of his case, XYZ’s attorney has served us with a subpoena requesting a copy of the tape of his internal disciplinary proceeding, for use as potential evidence. A copy of that subpoena is enclosed.

The tape that XYZ has requested can be obtained by subpoena, which is a routine process in litigation, but, in accordance with the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, you are entitled to notice in advance of our response because of your involvement in the hearing either as a member of the disciplinary panel or as a witness (either in person or through a statement presented by one of the parties). You also have the right, at your option, to file an objection with the court if you believe that there is a legal basis that information concerning you should not be disclosed. We will provide a copy of the tape to XYZ’s counsel on July 7, as required by the subpoena, if no such objection has been filed.

It is possible that XYZ’s attorney will attempt to contact you at some point in the future to discuss his case. You are free to speak with him if you wish, but you are not required to do so.

If you have any questions about this matter, please feel free to contact me. As RISD’s in-house lawyer, I cannot give you legal advice or provide you with legal representation, but I will be happy to answer your questions as best I can.

Very truly yours,

Steven J. McDonald
General Counsel

Re: ABC v. XYZ

Dear Mr. Lawyer:

I have received the subpoena you issued to Rhode Island School of Design for the tape of the disciplinary hearing involving XYZ. I am writing to object to that subpoena pursuant to Civil Rule 45(C)(2)(b), on the grounds that the subpoena seeks disclosure of matter protected by federal law and does not allow reasonable time to comply.

The tape that you have requested contains the names of, and other personally identifiable information concerning, a number of our students and, as such, constitutes an “education record” under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g. In the absence of consent from each of those students, FERPA prohibits us from complying with your subpoena unless we first provide reasonable advance notice to each of them so that they may seek protective action should they so desire. 34 C.F.R. § 99.31(a)(9)(i)-(ii). While we assume that your client has consented to the release of his own information, we are not aware of any such consent from the remaining students. We therefore will proceed to provide the required notice to those students and will then provide you with a copy of the tape if none of them has filed a motion to quash within fourteen days.

Please feel free to contact me at 277-4955 if you would like to discuss this matter.

Very truly yours,

Steven J. McDonald
General Counsel

VIA FAX

XYZ

Assistant U.S. Attorney

Re: Federal Grand Jury Subpoena for Documents Pertaining to ABC

Dear Mr. XYZ:

I am writing in response to your letter of today reiterating your concerns about our compliance with the requirements of the Family Educational Rights and Privacy Act. Please be aware that, while we understand your policy concerns and fully agree with them, compliance with FERPA, a federal statute, is not optional for us. (The reason that the Department of Education did not raise FERPA in response to your subpoena is that FERPA does not apply to DOE.) In fact, we currently are subject to a federal court injunction specifically prohibiting us from releasing student records “except as . . . expressly permitted under FERPA”. *United States of America v. Miami University, et al.*, 91 F. Supp. 2d 1132, 1160 (S.D. Ohio 2000). Our intent in attempting to discuss this matter with you has been not to frustrate your investigation, but, rather, solely to find a way that we can accommodate your concerns without violating FERPA.

There are three options for proceeding at this point:

1. You can reissue your grand jury subpoena (or issue a new administrative one) stating on its face that the existence and contents of the subpoena should not be disclosed to Mr. ABC. *See* 34 C.F.R. § 99.31(a)(9)(ii)(A) and (B). Under the circumstances, this would appear to be the simplest solution.
2. You can make your request pursuant to 34 C.F.R. § 99.31(A)(3) and 34 C.F.R. § 99.35. In order to do so, however, you will need to withdraw your subpoena, make a separate request, and specifically advise us that you are making the request “in connection with . . . the enforcement of . . . Federal legal requirements which relate to” federal education programs, 34 C.F.R. § 99.35(a), not simply that it is “in the course of an ongoing federal criminal investigation of Mr. ABC”:

The statutory amendment provides for nonconsensual disclosure of education records to authorized representatives of the Attorney General for law enforcement purposes under the same conditions that apply to the Secretary. In the case of the Attorney General, “law enforcement purposes” refers to the investigation or enforcement of Federal legal requirements applicable to

federally supported education programs. For example, under this exception, the authorized representatives of the Attorney General can access education records without consent in order to investigate or enforce Title II of the Americans with Disabilities Act, Section 504 of the Rehabilitation Act of 1973, the Equal Educational Opportunities Act of 1974, Title IX of the Education Amendments of 1972, Title IV of the Civil Rights Act of 1964, or the Civil Rights of Institutionalized Persons Act (CRIPA). Authorized representatives of the Attorney General include any employee of the Department of Justice, including the Federal Bureau of Investigation, so long as the employee is authorized to investigate or enforce the Federal legal requirements applicable to federally supported education programs.

This exception does not supersede or modify the exception in Sec. 99.31(a)(9) for disclosure in compliance with a judicial order or lawfully issued subpoena. Rather, this new exception permits non-consensual disclosure of education records in connection with the Attorney General's investigation or enforcement of Federal legal requirements of federally supported education programs.

65 Fed. Reg. 41852, 41856 (July 6, 2000) (emphasis added).

3. We can comply with your subpoena as is, after providing notice to Mr. ABC in accordance with 34 C.F.R. § 99.31(a)(9)(ii).

We do not intend to resist your subpoena and, in fact, already have gathered the documents that you have requested. We also understand that you do not wish for us to proceed with option 3, and we would be happy to proceed with whichever of the other two options that you would prefer. Unless we have heard from you by this Friday, however, we will have no choice but to proceed with option 3. Even if Mr. ABC has no basis to seek to quash your subpoena, he nevertheless is entitled to reasonable advance notice, and the time frame under which you wish to proceed will leave us with no other choice, *see* <<http://www.ed.gov/offices/OM/OMltrs/Youngstown.html>>.

Very truly yours,

Steven J. McDonald
Associate Legal Counsel

What is FERPA?

The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects personally identifiable information (PII) in students' education records from unauthorized disclosure. It affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right for parents and eligible students to have some control over the disclosure of PII from education records.

FERPA includes provisions allowing students' PII from education records to be disclosed without the prior written consent of parents, if the disclosure meets the criteria for one of the permitted consent exceptions.

The school official exception allows educational agencies to share PII from education records without consent with contractors, consultants, volunteers, or other parties to whom an agency or institution has outsourced institutional services or functions, as long as certain additional requirements are met.

The FERPA statute is codified at 20 U.S.C. § 1232g, and the FERPA regulations are found at 34 CFR Part 99.

What are my responsibilities under [Name of State Statute]?

[Insert information about state requirements.]

Who can I contact for more information?

[Insert name of appropriate contact.]



Acknowledgement of Volunteer Responsibilities under the Family Educational Rights and Privacy Act (FERPA) [and] [Name of State Statute]

This document is intended for Local Education Agencies (LEAs) and schools to give to their volunteers to inform them about their responsibilities to protect students' personally identifiable information from education records acquired under FERPA's school official exception. For more information about FERPA, please visit <http://ptac.ed.gov> and <http://familypolicy.ed.gov>.



Introduction

You have volunteered for **[name of school/district]** to perform services that require you to access and use personally identifiable information (PII) from students' education records. Your access and use of the PII is governed by the Family Educational Rights and Privacy Act (FERPA).

FERPA requires the school or school district to maintain "direct control" over your use and maintenance of students' education records and to use reasonable methods to ensure that you obtain access to only those education records in which you have an educational interest.

If you have any questions about information in this document, they should be directed to [point of contact for your school or school district].



What should I do to protect student PII from education records under FERPA?

It's important that you take the following steps to protect student privacy:

- *Do not disclose the PII to another party (except back to the School or District). The PII must not be shared with unauthorized users, and it must be protected from inadvertent disclosure due to careless handling.*
- *Do not use the PII for other purposes. The PII has been provided only for you to perform the volunteer service for which the school provided you the information. It should not be used for other purposes.*
- *Do not keep the PII after you complete your volunteer service. Destroy or return the PII to the school or district after completion of the service that you provided.*

The undersigned acknowledges that he or she has read, understands, and will uphold all responsibilities as outlined in *Acknowledgement of Volunteer Responsibilities under FERPA*.

(Print name)

(Name of school or school district)

(Signature)

(Date)



Model Notification of Rights under FERPA for Postsecondary Institutions

The Family Educational Rights and Privacy Act (FERPA) afford eligible students certain rights with respect to their education records. (An “eligible student” under FERPA is a student who is 18 years of age or older or who attends a postsecondary institution.) These rights include:

1. The right to inspect and review the student's education records within 45 days after the day the [Name of postsecondary institution (“School”)] receives a request for access. A student should submit to the registrar, dean, head of the academic department, or other appropriate official, a written request that identifies the record(s) the student wishes to inspect. The school official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the school official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.
2. The right to request the amendment of the student’s education records that the student believes is inaccurate, misleading, or otherwise in violation of the student’s privacy rights under FERPA.

A student who wishes to ask the school to amend a record should write the school official responsible for the record, clearly identify the part of the record the student wants changed, and specify why it should be changed.

If the school decides not to amend the record as requested, the school will notify the student in writing of the decision and the student’s right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.

3. The right to provide written consent before the university discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent.

The school discloses education records without a student’s prior written consent under the FERPA exception for disclosure to school officials with legitimate educational interests. A school official is a person employed by the [School] in an administrative, supervisory, academic, research, or support staff position (including law enforcement unit personnel and health staff); a person serving on the board of trustees; or a student serving on an official committee, such as a disciplinary or grievance committee. A school official also may include a volunteer or contractor outside of the [School] who performs an institutional service of function for which the school would otherwise use its own employees and who is under the direct control of the school with respect to the use and maintenance of PII from education records, such as an attorney, auditor, or collection agent or a student volunteering to assist another school official in performing his or her tasks. A school official has a

legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibilities for the [School].

[Optional] Upon request, the school also discloses education records without consent to officials of another school in which a student seeks or intends to enroll. [NOTE TO POSTSECONDARY INSTITUTION: FERPA requires a school to make a reasonable attempt to notify each student of these disclosures unless the school states in its annual notification that it intends to forward records on request.]

4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the [School] to comply with the requirements of FERPA. The name and address of the Office that administers FERPA is:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, DC 20202

[NOTE: In addition, a school may want to include its directory information public notice, as required by §99.37 of the regulations, with its annual notification of rights under FERPA.]

[Optional] See the list below of the disclosures that postsecondary institutions may make without consent.

FERPA permits the disclosure of PII from students' education records, without consent of the student, if the disclosure meets certain conditions found in §99.31 of the FERPA regulations. Except for disclosures to school officials, disclosures related to some judicial orders or lawfully issued subpoenas, disclosures of directory information, and disclosures to the student, §99.32 of FERPA regulations requires the institution to record the disclosure. Eligible students have a right to inspect and review the record of disclosures. A postsecondary institution may disclose PII from the education records without obtaining prior written consent of the student –

- To other school officials, including teachers, within the [School] whom the school has determined to have legitimate educational interests. This includes contractors, consultants, volunteers, or other parties to whom the school has outsourced institutional services or functions, provided that the conditions listed in §99.31(a)(1)(i)(B)(1) - (a)(1)(i)(B)(2) are met. (§99.31(a)(1))
- To officials of another school where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of §99.34. (§99.31(a)(2))
- To authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as a State postsecondary authority that is responsible for supervising the university's State-supported education programs. Disclosures under this provision may be made, subject to the requirements of §99.35, in connection with an audit or

evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. These entities may make further disclosures of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf. (§§99.31(a)(3) and 99.35)

- In connection with financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid. (§99.31(a)(4))
- To organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction. (§99.31(a)(6))
- To accrediting organizations to carry out their accrediting functions. (§99.31(a)(7))
- To parents of an eligible student if the student is a dependent for IRS tax purposes. (§99.31(a)(8))
- To comply with a judicial order or lawfully issued subpoena. (§99.31(a)(9))
- To appropriate officials in connection with a health or safety emergency, subject to §99.36. (§99.31(a)(10))
- Information the school has designated as “directory information” under §99.37. (§99.31(a)(11))
- To a victim of an alleged perpetrator of a crime of violence or a non-forcible sex offense, subject to the requirements of §99.39. The disclosure may only include the final results of the disciplinary proceeding with respect to that alleged crime or offense, regardless of the finding. (§99.31(a)(13))
- To the general public, the final results of a disciplinary proceeding, subject to the requirements of §99.39, if the school determines the student is an alleged perpetrator of a crime of violence or non-forcible sex offense and the student has committed a violation of the school’s rules or policies with respect to the allegation made against him or her. (§99.31(a)(14))
- To parents of a student regarding the student’s violation of any Federal, State, or local law, or of any rule or policy of the school, governing the use or possession of alcohol or a controlled substance if the school determines the student committed a disciplinary violation and the student is under the age of 21. (§99.31(a)(15))



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/fpc>.

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\(a\)\(1\)](#).



Protecting Student Privacy While Using Online Educational Services: Model Terms of Service

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 of this Guidance

In February 2014, PTAC issued guidance titled [*Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*](#). This *Model Terms of Service* document is intended to further assist schools and school districts in implementing that guidance.

In a traditional contracting process, the buyer and seller mutually agree on a set of terms and then sign a contract reflecting those terms. However, many providers of online educational services and mobile applications (i.e., vendors, contractors, and other service providers) instead rely on a Terms of Service (TOS) agreement that requires a user to click to accept the agreement in order to access the service or application for the first time. These types of agreements are commonly referred to as “Click-Wrap” agreements. Once a user at the school or district clicks “I agree,” these terms will likely govern what information the provider may collect from or about students, what they can do with that information, and with whom they may share it. Depending on the content, Click-Wrap agreements may lead to violations 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.

PTAC offers this guidance to schools and districts to help them evaluate potential TOS agreements, and to offer direction regarding terminology frequently used in these agreements. By understanding commonly used provisions, schools and districts will be better able to decide whether to consent to a Click-Wrap or other TOS agreement for online educational services and mobile applications. The best practice recommendations below may also assist providers by suggesting approaches that better protect student privacy.

Schools and districts should exercise diligence when reviewing TOS agreements and follow established school and district policies for evaluating and approving online educational services and mobile applications. This will help ensure that the service or application is inventoried and evaluated, supports the school’s and district’s



broader mission and goals, and that the TOS is legally appropriate and compatible with the school’s and district’s policies and procedures.

Terms of Service and Privacy

When negotiating a contract or evaluating a provider’s TOS agreement, remember your school’s or district’s obligations regarding student privacy. Make sure the agreement explicitly describes how the provider may use and share student data.

The table below summarizes PTAC recommendations regarding key TOS provisions. The “GOOD!” column contains our best practice recommendations for TOS privacy provisions. If you see this language in your TOS, it is a positive indication that the provider is making a good faith effort to respect privacy. The “WARNING!” column contains provisions that represent poor privacy policy and may lead to violations of FERPA or other statutes. While these provisions are based on terms that may actually be used in providers’ TOS or privacy policies, they are presented here solely as illustrations of the types of provisions to look for while performing your own reviews of a provider’s privacy TOS. Actual TOS may have strong privacy protections that differ from those detailed below. As few TOS agreements will be worded exactly like the “GOOD!” or the “WARNING!” column, the final “Explanation” column provides context to help you interpret the rationale behind the provisions.

Privacy-Related Terms of Service Provisions

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
1	Definition of “Data”	“Data include all Personally Identifiable Information (PII) and other non-public information. Data include, but are not limited to, student data, metadata, and user content.”	<i>Beware of provisions that limit the definition of protected data:</i> “Data only include user information knowingly provided in the course of using (this service).”	The definition of data should include a broad range of information to which providers may have access in order to ensure as much information as possible is protected in the agreement. Beware of provisions that narrowly define the “Data,” “Student Information,” or “Personally Identifiable Information” that will be protected.



	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
2	Data De-Identification	<p>“Provider may use de-identified Data for product development, research, or other purposes. De-identified Data will have all direct and indirect personal identifiers removed. This includes, but is not limited to, name, ID numbers, date of birth, demographic information, location information, and school ID. Furthermore, Provider agrees not to attempt to re-identify de-identified Data and not to transfer de-identified Data to any party unless that party agrees not to attempt re-identification.”</p>	<p><i>Beware of provisions that define de-identification narrowly (as only the removal of direct identifiers, such as names and ID numbers) or lack a commitment from Providers to not re-identify the Data:</i></p> <p>“Provider may use de-identified Data for product development, research, or other purposes. De-identified Data will have all names and ID numbers removed.”</p>	<p>There is nothing wrong with a provider using de-identified data for other purposes; privacy statutes, after all, govern PII, not de-identified data. But because it can be difficult to fully de-identify data, as a best practice, the agreement should prohibit re-identification and any future data transfers unless the transferee also agrees not to attempt re-identification.</p> <p>It is also a best practice to be specific about the de-identification process. De-identification typically requires more than just removing any obvious individual identifiers, as other demographic or contextual information can often be used to re-identify specific individuals. Retaining location and school information can also greatly increase the risk of re-identification.</p>



	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
3	Marketing and Advertising	<p>“Provider will not use any Data to advertise or market to students or their parents. Advertising or marketing may be directed to the [School/District] only if student information is properly de-identified.”</p> <p><i>Or</i></p> <p>“Data may not be used for any purpose other than the specific purpose(s) outlined in this Agreement.”</p> <p><i>(If this provision is present, check to make certain there is nothing else in the agreement that would allow marketing/advertising).</i></p>	<p>“Provider may use Data to market or advertise to students or their parents.”</p>	<p>The TOS should be clear that data and/or metadata may not be used to create user profiles for the purposes of targeting students or their parents for advertising and marketing, which could violate privacy laws.</p>
4	Modification of Terms of Service	<p>“Provider will not change how Data are collected, used, or shared under the terms of this Agreement in any way without advance notice to and consent from the [School/District].”</p>	<p>“Provider may modify the terms of this Agreement at any time without notice to or consent from the [School/District].”</p> <p><i>Or</i></p> <p>“Provider will only notify the [School/District] of material changes.”</p>	<p>Schools/districts should maintain control of the data by preventing the provider from changing its TOS without the school’s/district’s consent.</p> <p>A provider that agrees to give notice of TOS changes is good; a provider that agrees not to change the TOS without consent is better.</p>



	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
5	Data Collection	“Provider will only collect Data necessary to fulfill its duties as outlined in this Agreement.”	<i>An absence of a data collection restriction (see left) could potentially allow vendors to collect a wide array of student information. Also watch for:</i> “If user gains access through a third-party website (such as a social networking site), personal information associated with that site may be collected.”	If the agreement relates to FERPA-protected data, a provision like the one represented in the “GOOD!” column may be necessary. Including a provision that limits data collection to only what is necessary to fulfill the agreement is a best practice. Providers may view user access to their services through a third-party social networking site as an exception to established rules limiting data collection.
6	Data Use	“Provider will use Data only for the purpose of fulfilling its duties and providing services under this Agreement, and for improving services under this Agreement.”	<i>Beware of any provision that contains the phrase:</i> “without providing notice to users.”	Schools/districts should restrict data use to only the purposes outlined in the agreement. This will help schools/districts maintain control over the use of FERPA-protected student information and ensure appropriate data use.
7	Data Mining	“Provider is prohibited from mining Data for any purposes other than those agreed to by the parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited.”	“Provider can mine or scan Data and user content for the purpose of advertising or marketing to students or their parents.”	While data mining or scanning may sometimes be a necessary component of online services (e.g., for malware/spam detection or personalization tools), schools/districts should prohibit any mining or scanning for targeted advertising directed to students or their parents. Such provisions could lead to a violation of FERPA or the PPRA.



	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
8	Data Sharing	<p>“Data cannot be shared with any additional parties without prior written consent of the User except as required by law.”</p> <p><i>Or</i></p> <p>“The [School/District] understands that Provider will rely on one or more subcontractors to perform services under this Agreement. Provider agrees to share the names of these subcontractors with User upon request. All subcontractors and successor entities of Provider will be subject to the terms of this Agreement.”</p>	<p>“Provider may share information with one or more subcontractors without notice to User.”</p> <p><i>Or</i></p> <p>“Where feasible, Provider will require third-party vendors to comply with these Terms of Service.”</p>	While it is perfectly acceptable for providers to use subcontractors, schools/districts should be made aware of these arrangements and subcontractors should be bound by the limitations in the TOS.
9	Data Transfer or Destruction	<p>“Provider will ensure that all Data in its possession and in the possession of any subcontractors, or agents to which the Provider may have transferred Data, are destroyed or transferred to the [School/District] under the direction of the [School/District] when the Data are no longer needed for their specified purpose, at the request of the [School/District].”</p>	<p><i>Beware of any provision that contains:</i></p> <p>“maintain(s) the right to use Data or user content.”</p>	While FERPA does not specify that education records shared under some of its exceptions must be returned or destroyed at the end of the contract, it is a best practice to require this. Data return or destruction helps limit the amount of personal information available to third parties and prevent improper disclosure. This provision also helps schools/districts maintain control over the appropriate use and maintenance of FERPA-protected student information.



	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
10	Rights and License in and to Data	“Parties agree that all rights, including all intellectual property rights, shall remain the exclusive property of the [School/District], and Provider has a limited, nonexclusive license solely for the purpose of performing its obligations as outlined in the Agreement. This Agreement does not give Provider any rights, implied or otherwise, to Data, content, or intellectual property, except as expressly stated in the Agreement. This includes the right to sell or trade Data.”	“Providing Data or user content grants Provider an irrevocable right to license, distribute, transmit, or publicly display Data or user content.”	Maintaining ownership of data to which the provider may have access allows schools/districts to retain control over the use and maintenance of FERPA-protected student information. The “GOOD!” provision will also protect against a provider selling information.
11	Access	“Any Data held by Provider will be made available to the [School/District] upon request by the [School/District].”	<i>Beware of any provision that would limit the school’s or district’s access to the Data held by Provider.</i>	FERPA requires schools/districts to make education records accessible to parents. A good contract will acknowledge the need to share student information with the school upon request in order to satisfy FERPA’s parental access requirements. As a best practice, parental access to their children’s data should be seamless.



	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
12	Security Controls	“Provider will store and process Data in accordance with industry best practices. This includes appropriate administrative, physical, and technical safeguards to secure Data from unauthorized access, disclosure, and use. Provider will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Provider will also have a written incident response plan, to include prompt notification of the [School/District] in the event of a security or privacy incident, as well as best practices for responding to a breach of PII. Provider agrees to share its incident response plan upon request.”	<i>The lack of a security controls provision, or inclusion of a provision that sets a lower standard for Provider’s security of Data, would be a bad practice and potentially violate FERPA.</i>	Failure to provide adequate security to students’ PII is not a best practice and could lead to a FERPA violation.



Resources

Materials below include links to PTAC and other resources that provide additional best practice recommendations and guidance relating to TOS agreements. Please note that these resources do not necessarily address particular legal requirements (including FERPA requirements) that your school or district needs 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 applicable federal, state, tribal, and local requirements prior to entering into contractual agreements with providers.

Department of Education Resources

- Privacy Technical Assistance Center, U.S. Department of Education: <http://ptac.ed.gov>
- Privacy Technical Assistance Center, U.S. Department of Education, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* (2014): [http://ptac.ed.gov/sites/default/files/Student Privacy and Online Educational Services %28February 2014%29.pdf](http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20February%202014%29.pdf)
- Privacy Technical Assistance Center, U.S. Department of Education, *Written Agreement Checklist* (2012): http://ptac.ed.gov/sites/default/files/Written_Agreement_Checklist_0.pdf
- Family Policy Compliance Office, U.S. Department of Education: <http://familypolicy.ed.gov>

Other Government Resources

- FTC: Bureau of Consumer Protection Business Center, *Complying with COPPA: Frequently Asked Questions*: <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>
- National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing* (2011): <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf>



Protecting Student Privacy While Using Online Educational Services: Model Terms of Service

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 of this Guidance

In February 2014, PTAC issued guidance titled [*Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*](#). This *Model Terms of Service* document is intended to further assist schools and school districts in implementing that guidance.

In a traditional contracting process, the buyer and seller mutually agree on a set of terms and then sign a contract reflecting those terms. However, many providers of online educational services and mobile applications (i.e., vendors, contractors, and other service providers) instead rely on a Terms of Service (TOS) agreement that requires a user to click to accept the agreement in order to access the service or application for the first time. These types of agreements are commonly referred to as “Click-Wrap” agreements. Once a user at the school or district clicks “I agree,” these terms will likely govern what information the provider may collect from or about students, what they can do with that information, and with whom they may share it. Depending on the content, Click-Wrap agreements may lead to violations 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.

PTAC offers this guidance to schools and districts to help them evaluate potential TOS agreements, and to offer direction regarding terminology frequently used in these agreements. By understanding commonly used provisions, schools and districts will be better able to decide whether to consent to a Click-Wrap or other TOS agreement for online educational services and mobile applications. The best practice recommendations below may also assist providers by suggesting approaches that better protect student privacy.

Schools and districts should exercise diligence when reviewing TOS agreements and follow established school and district policies for evaluating and approving online educational services and mobile applications. This will help ensure that the service or application is inventoried and evaluated, supports the school’s and district’s



broader mission and goals, and that the TOS is legally appropriate and compatible with the school’s and district’s policies and procedures.

Terms of Service and Privacy

When negotiating a contract or evaluating a provider’s TOS agreement, remember your school’s or district’s obligations regarding student privacy. Make sure the agreement explicitly describes how the provider may use and share student data.

The table below summarizes PTAC recommendations regarding key TOS provisions. The “GOOD!” column contains our best practice recommendations for TOS privacy provisions. If you see this language in your TOS, it is a positive indication that the provider is making a good faith effort to respect privacy. The “WARNING!” column contains provisions that represent poor privacy policy and may lead to violations of FERPA or other statutes. While these provisions are based on terms that may actually be used in providers’ TOS or privacy policies, they are presented here solely as illustrations of the types of provisions to look for while performing your own reviews of a provider’s privacy TOS. Actual TOS may have strong privacy protections that differ from those detailed below. As few TOS agreements will be worded exactly like the “GOOD!” or the “WARNING!” column, the final “Explanation” column provides context to help you interpret the rationale behind the provisions.

Privacy-Related Terms of Service Provisions

	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
1	Definition of “Data”	“Data include all Personally Identifiable Information (PII) and other non-public information. Data include, but are not limited to, student data, metadata, and user content.”	<i>Beware of provisions that limit the definition of protected data:</i> “Data only include user information knowingly provided in the course of using (this service).”	The definition of data should include a broad range of information to which providers may have access in order to ensure as much information as possible is protected in the agreement. Beware of provisions that narrowly define the “Data,” “Student Information,” or “Personally Identifiable Information” that will be protected.



	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
2	Data De-Identification	<p>“Provider may use de-identified Data for product development, research, or other purposes. De-identified Data will have all direct and indirect personal identifiers removed. This includes, but is not limited to, name, ID numbers, date of birth, demographic information, location information, and school ID. Furthermore, Provider agrees not to attempt to re-identify de-identified Data and not to transfer de-identified Data to any party unless that party agrees not to attempt re-identification.”</p>	<p><i>Beware of provisions that define de-identification narrowly (as only the removal of direct identifiers, such as names and ID numbers) or lack a commitment from Providers to not re-identify the Data:</i></p> <p>“Provider may use de-identified Data for product development, research, or other purposes. De-identified Data will have all names and ID numbers removed.”</p>	<p>There is nothing wrong with a provider using de-identified data for other purposes; privacy statutes, after all, govern PII, not de-identified data. But because it can be difficult to fully de-identify data, as a best practice, the agreement should prohibit re-identification and any future data transfers unless the transferee also agrees not to attempt re-identification.</p> <p>It is also a best practice to be specific about the de-identification process. De-identification typically requires more than just removing any obvious individual identifiers, as other demographic or contextual information can often be used to re-identify specific individuals. Retaining location and school information can also greatly increase the risk of re-identification.</p>



	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
3	Marketing and Advertising	<p>“Provider will not use any Data to advertise or market to students or their parents. Advertising or marketing may be directed to the [School/District] only if student information is properly de-identified.”</p> <p><i>Or</i></p> <p>“Data may not be used for any purpose other than the specific purpose(s) outlined in this Agreement.”</p> <p><i>(If this provision is present, check to make certain there is nothing else in the agreement that would allow marketing/advertising).</i></p>	<p>“Provider may use Data to market or advertise to students or their parents.”</p>	<p>The TOS should be clear that data and/or metadata may not be used to create user profiles for the purposes of targeting students or their parents for advertising and marketing, which could violate privacy laws.</p>
4	Modification of Terms of Service	<p>“Provider will not change how Data are collected, used, or shared under the terms of this Agreement in any way without advance notice to and consent from the [School/District].”</p>	<p>“Provider may modify the terms of this Agreement at any time without notice to or consent from the [School/District].”</p> <p><i>Or</i></p> <p>“Provider will only notify the [School/District] of material changes.”</p>	<p>Schools/districts should maintain control of the data by preventing the provider from changing its TOS without the school’s/district’s consent.</p> <p>A provider that agrees to give notice of TOS changes is good; a provider that agrees not to change the TOS without consent is better.</p>



	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
5	Data Collection	“Provider will only collect Data necessary to fulfill its duties as outlined in this Agreement.”	<i>An absence of a data collection restriction (see left) could potentially allow vendors to collect a wide array of student information. Also watch for:</i> “If user gains access through a third-party website (such as a social networking site), personal information associated with that site may be collected.”	If the agreement relates to FERPA-protected data, a provision like the one represented in the “GOOD!” column may be necessary. Including a provision that limits data collection to only what is necessary to fulfill the agreement is a best practice. Providers may view user access to their services through a third-party social networking site as an exception to established rules limiting data collection.
6	Data Use	“Provider will use Data only for the purpose of fulfilling its duties and providing services under this Agreement, and for improving services under this Agreement.”	<i>Beware of any provision that contains the phrase:</i> “without providing notice to users.”	Schools/districts should restrict data use to only the purposes outlined in the agreement. This will help schools/districts maintain control over the use of FERPA-protected student information and ensure appropriate data use.
7	Data Mining	“Provider is prohibited from mining Data for any purposes other than those agreed to by the parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited.”	“Provider can mine or scan Data and user content for the purpose of advertising or marketing to students or their parents.”	While data mining or scanning may sometimes be a necessary component of online services (e.g., for malware/spam detection or personalization tools), schools/districts should prohibit any mining or scanning for targeted advertising directed to students or their parents. Such provisions could lead to a violation of FERPA or the PPRA.



	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
8	Data Sharing	<p>“Data cannot be shared with any additional parties without prior written consent of the User except as required by law.”</p> <p><i>Or</i></p> <p>“The [School/District] understands that Provider will rely on one or more subcontractors to perform services under this Agreement. Provider agrees to share the names of these subcontractors with User upon request. All subcontractors and successor entities of Provider will be subject to the terms of this Agreement.”</p>	<p>“Provider may share information with one or more subcontractors without notice to User.”</p> <p><i>Or</i></p> <p>“Where feasible, Provider will require third-party vendors to comply with these Terms of Service.”</p>	While it is perfectly acceptable for providers to use subcontractors, schools/districts should be made aware of these arrangements and subcontractors should be bound by the limitations in the TOS.
9	Data Transfer or Destruction	<p>“Provider will ensure that all Data in its possession and in the possession of any subcontractors, or agents to which the Provider may have transferred Data, are destroyed or transferred to the [School/District] under the direction of the [School/District] when the Data are no longer needed for their specified purpose, at the request of the [School/District].”</p>	<p><i>Beware of any provision that contains:</i></p> <p>“maintain(s) the right to use Data or user content.”</p>	While FERPA does not specify that education records shared under some of its exceptions must be returned or destroyed at the end of the contract, it is a best practice to require this. Data return or destruction helps limit the amount of personal information available to third parties and prevent improper disclosure. This provision also helps schools/districts maintain control over the appropriate use and maintenance of FERPA-protected student information.



	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
10	Rights and License in and to Data	“Parties agree that all rights, including all intellectual property rights, shall remain the exclusive property of the [School/District], and Provider has a limited, nonexclusive license solely for the purpose of performing its obligations as outlined in the Agreement. This Agreement does not give Provider any rights, implied or otherwise, to Data, content, or intellectual property, except as expressly stated in the Agreement. This includes the right to sell or trade Data.”	“Providing Data or user content grants Provider an irrevocable right to license, distribute, transmit, or publicly display Data or user content.”	Maintaining ownership of data to which the provider may have access allows schools/districts to retain control over the use and maintenance of FERPA-protected student information. The “GOOD!” provision will also protect against a provider selling information.
11	Access	“Any Data held by Provider will be made available to the [School/District] upon request by the [School/District].”	<i>Beware of any provision that would limit the school’s or district’s access to the Data held by Provider.</i>	FERPA requires schools/districts to make education records accessible to parents. A good contract will acknowledge the need to share student information with the school upon request in order to satisfy FERPA’s parental access requirements. As a best practice, parental access to their children’s data should be seamless.



	Provision	GOOD! This is a Best Practice	WARNING! Provisions That Cannot or Should Not Be Included in TOS	Explanation
12	Security Controls	<p>“Provider will store and process Data in accordance with industry best practices. This includes appropriate administrative, physical, and technical safeguards to secure Data from unauthorized access, disclosure, and use. Provider will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Provider will also have a written incident response plan, to include prompt notification of the [School/District] in the event of a security or privacy incident, as well as best practices for responding to a breach of PII. Provider agrees to share its incident response plan upon request.”</p>	<p><i>The lack of a security controls provision, or inclusion of a provision that sets a lower standard for Provider’s security of Data, would be a bad practice and potentially violate FERPA.</i></p>	<p>Failure to provide adequate security to students’ PII is not a best practice and could lead to a FERPA violation.</p>



Resources

Materials below include links to PTAC and other resources that provide additional best practice recommendations and guidance relating to TOS agreements. Please note that these resources do not necessarily address particular legal requirements (including FERPA requirements) that your school or district needs 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 applicable federal, state, tribal, and local requirements prior to entering into contractual agreements with providers.

Department of Education Resources

- Privacy Technical Assistance Center, U.S. Department of Education: <http://ptac.ed.gov>
- Privacy Technical Assistance Center, U.S. Department of Education, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* (2014): [http://ptac.ed.gov/sites/default/files/Student Privacy and Online Educational Services %28February 2014%29.pdf](http://ptac.ed.gov/sites/default/files/Student%20Privacy%20and%20Online%20Educational%20Services%20February%202014%29.pdf)
- Privacy Technical Assistance Center, U.S. Department of Education, *Written Agreement Checklist* (2012): http://ptac.ed.gov/sites/default/files/Written_Agreement_Checklist_0.pdf
- Family Policy Compliance Office, U.S. Department of Education: <http://familypolicy.ed.gov>

Other Government Resources

- FTC: Bureau of Consumer Protection Business Center, *Complying with COPPA: Frequently Asked Questions*: <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>
- National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing* (2011): <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf>



Best Practices for Data Destruction

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 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

Educational agencies and institutions increasingly collect and maintain large amounts of data about students in order to provide educational services. Some data, like students’ transcript information, may need to be preserved indefinitely. Other student information will need to be preserved for a prescribed period of time to comply with legal or policy requirements governing record retention, then will need to be destroyed once those time periods have elapsed. But a large amount of student information – some of which may still be highly sensitive – may become unnecessary or irrelevant the moment a student graduates or otherwise leaves the school, and can be destroyed immediately. Similarly, third parties providing services to a school or district, or conducting research or evaluations for a state or local educational agency, are often authorized to receive and use student data, but are typically required (either by law or by contract provisions) to destroy the student data when it is no longer needed for the specified purpose.

In most of these cases, merely deleting a digital record or file will be insufficient to destroy the information contained therein – as the underlying digital data are typically preserved in the system, and can often be “undeleted.” Specific technical methods used to dispose of the data greatly impact the likelihood that any information might be recovered.

This document will provide an overview of various methods for disposing of electronic data, and will discuss how these methods relate to legal requirements and established best practices for protecting student information.

Legal Requirements

The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the confidentiality of student information. FERPA protects personally identifiable information (PII) from students' education records from disclosure without written consent from the parent or "eligible student" (a student who is 18 years of age, or who is attending a post-secondary institution), unless an exception to that consent requirement applies. For a detailed explanation of FERPA, the various exceptions to the consent requirement, and the requirements and conditions for each, please visit the PTAC website at <http://ptac.ed.gov>.

FERPA does not provide any specific requirements for educational agencies and institutions regarding disposition or destruction of the data they collect or maintain themselves, other than requiring them to safeguard FERPA-protected data from unauthorized disclosure, and not to destroy any education records if there is an outstanding request to inspect or review them. When educational agencies and institutions disclose (or "share") PII from education records with third parties under an applicable exception to FERPA's written consent requirement, however, additional legal requirements regarding destruction of that PII may apply.

Under the "school official" exception, FERPA requires that the school or district maintain direct control over the authorized recipient's maintenance and use of the PII from education records, and that the recipient protect the PII from further or unauthorized disclosure. While these general requirements for protection of and direct control over the maintenance of the PII imply adequate destruction of that PII when no longer needed, FERPA's school official exception leaves it to the educational agency or institution to establish specific terms for the protection of and direct control over the maintenance of the PII from education records (including its eventual destruction).

Two commonly used exceptions to FERPA's written consent requirement provide more specificity regarding data destruction. FERPA's "studies" and "audit or evaluation" exceptions require the disclosing agency or institution to enter into a written agreement with the third party receiving the PII from education records. Under these exceptions, the agreement must (among other things) specify that the PII must be destroyed when no longer needed for the specific purpose for which it was disclosed and a time period for that destruction. While FERPA does not provide any technical standards for destruction, the audit or evaluation exception does require that the disclosing entity use "reasonable methods" to ensure that the PII from education records is properly protected by the recipient. (For more information on these two exceptions, the other requirements for written agreements, or additional guidance on what constitutes "reasonable methods," visit the PTAC website at <http://ptac.ed.gov>).

While FERPA is silent on specific technical requirements governing data destruction, methods discussed in this document should be viewed as best practice recommendations for educational agencies and institutions to consider adopting when establishing record retention and data

governance policies to follow internally, and also for inclusion in any written agreements and contracts they make with third parties to whom they are disclosing PII.

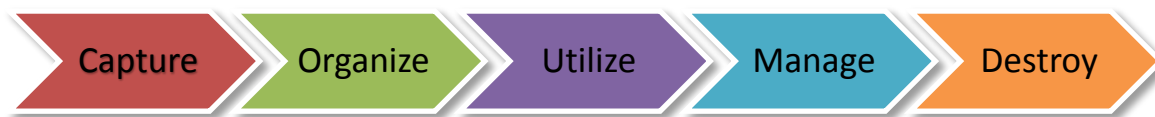
It should also be noted that while FERPA does not require that particular methods of data destruction be used, other applicable Federal, State, or local privacy laws and regulations may require specific secure data disposal methods. When creating data sharing agreements, check with your legal counsel to fully understand what requirements apply and how to proceed.

Depending on the type of data involved and the context in which the data are being used, there may be a number of specific requirements with which educational agencies and institutions must comply. For example, Part B of the Individuals with Disabilities Education Act (IDEA) requires public agencies to inform a student’s parents when any PII collected, maintained, or used thereunder is no longer needed to provide educational services to the child. Subsequently, the information must be destroyed at the request of the parents (though a permanent record of a student's name, address, and phone number, his or her grades, attendance record, classes attended, grade level completed, and year completed may be maintained without time limitation. 34 CFR § 300.624(a) and (b)). Part B of the IDEA defines the term “destruction” as the “physical destruction or removal of personal identifiers from information so that the information is no longer personally identifiable.” 34 CFR § 300.611(a)

Lastly, methods discussed in this guidance are intended as examples and should not be considered to be exhaustive. More detailed technical information can be found in the [National Institute of Standards and Technology \(NIST\) Special Publication 800-88 Rev. 1 \(Draft\): Guidelines for Media Sanitization](#).

What is Data Destruction?

Data should be appropriately managed across the entire data lifecycle, from capture to destruction. Planning for data destruction is an integral part of a high quality data management program.



Data Lifecycle

Data in any of their forms move through stages during their useful life and ultimately are either archived for later use, or destroyed when their utility has been exhausted. Establishing policies and procedures governing the management and use of data allows an organization to more efficiently and

safely protect its data (see PTAC's resources on Data Governance at <http://ptac.ed.gov>). When data are no longer needed, the destruction of the data becomes a critical, and often required, component of an effective data governance program. Data destruction is the process of removing information in a way that renders it unreadable (for paper records) or irretrievable (for digital records).

Because some methods of data destruction are more complicated, time-consuming, or resource intensive than others, it is common to select the method based on the underlying sensitivity of the data being destroyed, or the potential harm they could cause if they are recovered or inadvertently disclosed. For very low risk information, this may mean simply deleting electronic files or using a desk shredder for paper documents. However, these types of destruction methods can be undone, by a determined and motivated individual, making these methods inappropriate for more sensitive data. For more sensitive data, stronger methods of destruction at a more granular level may need to be employed to assure that the data are truly irretrievable.

How Long Should Data Be Retained Before They Are Destroyed?

FERPA does not require educational agencies and institutions to destroy education records maintained as a part of the regular school or agency operations, and in fact, many jurisdictions require lengthy retention periods for student attendance and graduation records. For other student records, in order to minimize information technology (IT) costs and reduce the likelihood of inadvertent disclosure of student information, schools and districts will often elect to establish their own record retention policies, including time frames for eventual destruction of the records. Minimizing the amount of data you retain, by destroying them when no longer needed, is a key element of the Fair Information Practice Principles (FIPPs), and is widely considered to be a best practice for protecting individuals' privacy and for lessening the potential impact of a data breach or inadvertent disclosure. For more information on FIPPs (including Data Minimization), see <http://www.nist.gov/nstic/NSTIC-FIPPs.pdf>.

Under the "studies" and "audit or evaluation" exceptions, FERPA requires that PII from education records be destroyed when no longer needed for the specific purpose for which it was disclosed, and that the written agreement specify the time period for destruction. When drafting these agreements, it may be difficult to accurately predict the appropriate destruction period in advance. In these cases, the parties may wish to consider establishing a time period for destruction of the PII, and then modifying the written agreement, if needed, to postpone the destruction date or move it sooner than initially specified. This can be especially important for longitudinal studies, which may span many decades. While FERPA requires that there be an end date upon which any PII from education records disclosed under the studies or audit or evaluation exception must be destroyed, it does not specify a maximum time limit. In determining the appropriate time frame for the destruction of PII for a given study or audit or evaluation, some important issues should be considered. For example, for the purposes of verification and repeatability of findings, it may not be feasible to immediately destroy all of the PII involved in a study. In these cases, consider adding provisions within the agreement for the retention of PII needed for repeatability for an additional specified length of time. Additionally, an

educational agency or institution might consider using a strategy in which the third party returns the research dataset to the educational agency or institution for archiving. In these cases, the third party would then destroy residual PII, leaving the educational agency or institution with the study dataset.

Under the school official exception, it is a best practice for schools and districts to require the third party receiving the PII to destroy it upon termination of the school official relationship (e.g., when the contract ends), or when no longer needed for the purpose for which it was disclosed (whichever comes first).

When PII from education records is disclosed under any of FERPA's other exceptions, unless legal requirements specify otherwise, it is a best practice for educational agencies and institutions to require the recipient to destroy the PII when no longer needed for the purpose for which it was disclosed.

Please note that other Federal, state, and local privacy laws and regulations may contain more stringent data retention and/or destruction requirements, so it is important to consider and comply with all applicable requirements when determining the appropriate time period for retention and destruction of data.

Best Practices for Data Destruction




The information below contains some common best practices for data destruction. This guidance should not be considered comprehensive. Many additional technologies and methodologies exist which may or may not apply to your specific needs. While this document provides high level recommendations, the National Institute of Standards and Technology (NIST) provides in-depth guidance and best practices for the implementation of effective methods of data destruction in their [Guidelines for Media Sanitation](#).

Modern electronic data storage devices are extremely resilient, and data recovery techniques and technology are highly advanced. Data are routinely recovered from media which have been burned, crushed, submerged in water, or impacted from great heights. In effect, it really is quite difficult to permanently get rid of data, but the permanent and irreversible destruction of data is a cornerstone of protecting the privacy and security of students' education records. Data destruction encompasses a wide variety of media, including electronic and paper records. The choice of destruction methodology should be based on the risk posed by the sensitivity of the data being destroyed and the potential impact of unauthorized disclosure. For example, the negative impact from the disclosure of a file containing directory information, such as names of honor roll students, might not be as severe as the negative impact from the disclosure of a file containing students' Social Security Numbers, names, and dates of birth. Therefore, the approach to data destruction in these two scenarios might be different. While the negative impact from the disclosure of de-identified data may warrant only their deletion from a disk or other media, the negative impact and risk of unauthorized disclosure of sensitive PII

typically would warrant stronger methods of data destruction. In the latter case, the organization might use a software or hardware technique that completely cleans the hard disk containing the PII to the point that the data cannot be retrieved, even forensically.

The table below identifies three major categories of data destruction. The table is arranged according to the degree of assurance each category provides, with “clear” providing the least amount of assurance and “destroy” providing the most assurance that the information is irretrievable. Organizations should make risk-based decisions on which method is most appropriate based on the data type, risk of disclosure, and the impact if that data were to be disclosed without authorization.

Data Destruction Categories

 Clear	<p>A method of sanitization that applies programmatic, software-based techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).</p>
 Purge	<p>A method of sanitization that applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.</p>
 Destroy	<p>A method of sanitization that renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.</p>

Adapted from NIST Draft Special Publication 800-88 Rev 1: Guidelines for Media Sanitization; Section 2.5 – Types of Sanitization

More information about the specific technical requirements for data destruction for various hardware and media types can be found in NIST's [Guidelines for Media Sanitation](#), Appendix A: "Minimum Sanitization Recommendations."

No matter which method of destruction you choose, consider following these general best practices for data destruction:

- ✓ When drafting written agreements with third parties, include provisions that specify that all PII that was provided to the third party must be destroyed when no longer needed for the specific purpose for which it was provided, including any copies of the PII that may reside in system backups, temporary files, or other storage media.
- ✓ Ensure accountability for destruction of PII by using certification forms which are signed by the individual responsible for performing the destruction and contain detailed information about the destruction.
- ✓ Remember that PII may also be present in non-electronic media. Organizations should manage non-electronic records in a similar fashion to their electronic data. When data are no longer required, destroy non-electronic media using secure means to render it safe for disposal or recycling. Commonly used methods include cross-cut shredders, pulverizers, and incinerators.
- ✓ Depending on the sensitivity of the data being shared, be specific in the written agreement as to the type of destruction to be carried out.
- ✓ When destroying electronic data, use appropriate data deletion methods to ensure the data cannot be recovered. Please note that simple deletion of the data is not effective. Often, when a data file is deleted, only the reference to that file is removed from the media. The actual file data remain on the disk and are available for recovery until overwritten. Talk to your IT professional to ensure proper deletion of records consistent with technology best practice standards.
- ✓ Avoid using file deletion, disk formatting, and "one way" encryption to dispose of sensitive data—these methods are not effective because they leave the majority of the data intact and vulnerable to being retrieved by a determined person with the right tools.
- ✓ Destroy CDs, DVDs, and any magneto-optical disks by pulverizing, cross-cut shredding, or burning.
- ✓ Address in a timely manner sanitization of storage media which might have failed and need to be replaced under warranty or service contract. Many data breaches result from storage media containing sensitive information being returned to the manufacturer for service or replacement.
- ✓ Create formal, documented processes for data destruction within your organization and require that partner organizations do the same.

Best Practices in Data Destruction – An Example

A school district wants to evaluate how its former elementary students are doing in its high school to improve its elementary school instruction. The district decides to contract with a research organization to perform a study to determine ways to improve instruction in its elementary school.

The district enters into a written agreement with the research organization under the FERPA studies exception. The agreement establishes clear guidelines and data management requirements to protect the privacy and confidentiality of the data, specifying that:

- ✓ the study will take eight months to complete,
- ✓ the data provided by the district are to be used only for the express purposes outlined in the study,
- ✓ the research organization must put in place controls to limit access to the data and use secure file transfer process in accordance with the industry's standards for strong encryption mechanisms, and
- ✓ the data will be destroyed when no longer needed to conduct the study and by the end of the eight month contract.

In addition, the district stipulates in the written agreement that at the end of the contract the research dataset used for the study will be securely returned to the district, which will archive the file in case it is needed for future replication or evaluation of the findings, and that any remaining district data held by the research organization must be destroyed. The written agreement also stipulates the specific data destruction method that the research organization will use: in this case, a secure overwrite utility that overwrites the data files with random information, thus rendering the entirety of the data unrecoverable.

The written agreement explicitly identifies the person within the research organization who is responsible for the data while they are being used for the study, and the individual accountable for their destruction at the end of the project. The agreement also includes a destruction certification form on which the research organization must inventory the data destruction efforts, to be signed by the person responsible for destroying the data.

At the end of the contract, the research organization securely returns the study dataset back to the district and conducts the destruction of any remaining data using the agreed-upon tool to overwrite the data. The destruction is annotated on the form provided by the district and signed by the individual responsible for the destruction. The transport media that the district provided to the research organization for the purposes of conducting the study are securely returned to the district with the completed verification form.

Additional Resources

The resources below include links to federal regulations and several guidance documents outlining security issues, best practices and methodologies, and frameworks for secure data destruction.

- Family Policy Compliance Office, U.S. Department of Education, *Guidance for Reasonable Methods and Written Agreements* (2011): www.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd_agreement.pdf
- National Institute of Standards and Technology (NIST), *Guide for Conducting Risk Assessments, SP 800-30 Rev. 1* (2012): http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
- National Institute of Standards and Technology (NIST), *Guidelines for Media Sanitization, Draft SP 800-88 Rev. 1* (2012): http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf
- National Institute of Standards and Technology (NIST), *Guide to Selecting Information Technology Security Products* (2003): <http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf>
- National Institute of Standards and Technology (NIST), *Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publication (FIPS PUB) 199* (2004): <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
- Privacy Technical Assistance Center (PTAC), U.S. Department of Education: <http://ptac.ed.gov>
- 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. Department of Education, *Family Educational Rights and Policy Act (FERPA) regulations amendment* (2011): www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf

Glossary

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](#).

Encryption is the process of transforming information using a cryptographic algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as an encryption/decryption key. “One way” encryption is a data destruction technique which makes use of encryption techniques to render data unusable by first encrypting the data and then destroying the key used to encrypt the data initially.

Personally identifiable information (PII) from education records includes information, such as a student’s name or identification number, that 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.

Sanitization of the media is a process which is applied to data or storage media to make data retrieval unlikely for a given level of effort. *Clear*, *Purge*, and *Destroy* are actions that can be taken to sanitize data and media.

Sensitive data are data that carry the risk for adverse effects from an unauthorized or inadvertent disclosure. This includes any negative or unwanted effects experienced by an individual whose personally identifiable information (PII) from education records was the subject of a loss of confidentiality that may be socially, physically, or financially damaging, as well as any adverse effects experienced by the organization that maintains the PII. See [Guide to Protecting the Confidentiality of Personally Identifiable Information \(PII\)](#), 2010, NIST Special Publication 800-122, for more information.