



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.

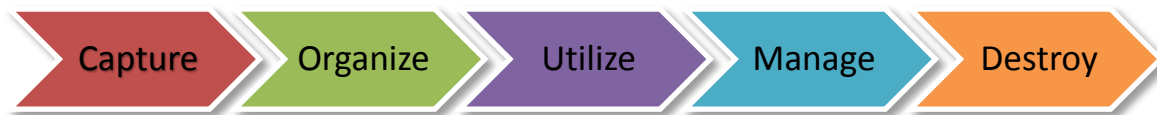
It should also be noted that while FERPA does not require that particular methods of data destruction be used, other applicable Federal, State, or local privacy laws and regulations may require specific secure data disposal methods. When creating data sharing agreements, check with your legal counsel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