



OSSE Shared Data Destruction Policy

Effective March 2019 | Last Updated April 23, 2025

I. Authority	The Office of the State Superintendent of Education (OSSE) adopts this policy to strengthen OSSE's data protection and privacy practices.
II. Applicability	This policy applies to third parties with which OSSE shares data under a written agreement (generally called a Data Sharing Agreement).
III. Rationale	To set requirements about the methods for and full scope of verifiable data destruction for all data shared by OSSE with third parties under a written agreement. This policy aligns with best practices recommended by the US Department of Education and under the Family Educational Rights and Privacy Act (FERPA).
IV. Policy	<p>This policy sets requirements for documentation of data destruction plans and their completion by third parties under a written agreement.</p> <p>Third parties are not permitted to retain any data from OSSE beyond the terms of a data sharing agreement.¹</p> <p>Under every data sharing agreement, the third party agrees to destroy all data shared:</p> <ul style="list-style-type: none">• At OSSE's request;• When the data are no longer needed to achieve the agreement's purpose;• Upon termination of the agreement; and/or• As otherwise required by State or Federal law. <p>Within seven days of the termination of an agreement, third parties must complete and sign an OSSE-provided certificate of data destruction attesting that all OSSE data shared under an agreement has been sanitized according to the Guidelines for Media Sanitization issued by the National Institute of Standards and Technology (NIST)².</p> <p>When entering into a data sharing agreement, third parties may propose alternative methods of data destruction for OSSE review but must justify in writing why they cannot follow the NIST guidelines.</p>

¹ If programmatic reasons continue to exist for the data sharing, agreements can be extended or otherwise modified to allow the work to continue.

² NIST Special Publication 800-88, Rev. 1. *Guidelines for Media Sanitization*.
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf>

	OSSE does not consider third-party de-identification as data destruction.
V. Definitions	<p>Data:</p> <ul style="list-style-type: none"> Expressed information representing facts in a variety of qualitative and quantitative forms, including aggregate, individual level, and personally identifiable information. <p>Data Files:</p> <ul style="list-style-type: none"> Data files are physical and electronic representations of information, and any copies made. Examples of data files include but are not limited to: <ul style="list-style-type: none"> Hard drives Cloud-based applications (e.g., Microsoft Share Point, Amazon Web Services, etc.) Networking equipment Paper printouts Flash drives Institutional servers Any other type of materials that store, capture, or process data <p>Personally Identifiable Information (PII):</p> <ul style="list-style-type: none"> PII is information that, alone or in combination with other data, can be linked to a specific child or student, including but not limited to: <ul style="list-style-type: none"> Name of child, student, parents, or other family members; Address of child, student, parents, or other family members; Personal identifier, such as a Social Security Number, unique student identifier (such as OSSE’s USI), or biometric record; and Indirect identifiers, such as date of birth, place of birth, or mother’s maiden name. <p>Data Sharing Agreement (DSA):</p> <ul style="list-style-type: none"> A legal document, signed by the Superintendent, authorizing OSSE to share specific data for a specific purpose with a third party in accordance with FERPA. <p>Data Destruction:</p> <ul style="list-style-type: none"> Data destruction, as required under FERPA, is the process of removing information in a way that renders it unreadable (for paper records) or irretrievable (for digital records).³ <p>Data Sanitization:</p> <ul style="list-style-type: none"> Data sanitization, as defined by NIST, refers to a process that renders access to target data infeasible for a given level of effort (purge, clear, destroy). All three actions are acceptable methods of FERPA-defined “data destruction,” and can be used interchangeably. <p>De-identification:</p>

³ Privacy Technical Assistance Center, <https://studentprivacy.ed.gov/resources/best-practices-data-destruction>

	<ul style="list-style-type: none"> De-identification of data refers to the process of removing or obscuring any PII from a dataset in a way that minimizes the risk of unintended disclosure of the identity of individuals and information about them. While it may not be possible to remove the disclosure risk completely, de-identification is considered successful when there is no reasonable basis to believe that the remaining information in the records can be used to identify any individual.⁴ <p>Third Party:</p> <ul style="list-style-type: none"> A third party is any entity external to OSSE that has no ownership of OSSE’s data, such as a researcher or another District of Columbia government agency.
VI. Auditing, Monitoring and Review	Under FERPA, and within the terms OSSE’s data sharing agreements, OSSE has the right to monitor a third party’s compliance with the documented process for data destruction.
VII. Consequences for Non-compliance	OSSE considers third parties retaining its data beyond the expiration date of a written agreement to be in breach of the agreement. In such cases, OSSE will take steps to require the third party to remediate the breach, come into compliance, and destroy the data as immediately as possible. Such steps may include issuing a compliance letter to the third party up to and including denial of access to OSSE data in the future, depending on the depth, duration, and severity of the breach.
VIII. Further Information	For more information on this policy or the data request, sharing, or destruction processes, please visit the Data Governance and Privacy at OSSE page or contact OSSE.datasharing@dc.gov .

⁴ As noted above, OSSE does not consider third-party de-identification as data destruction. US Department of Education, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms_0.pdf