DISTRICT OF COLUMBIA
OFFICE OF THE STATE SUPERINTENDENT OF
EDUCATION

SHARED DATA DESTRUCTION POLICY

Effective March 1, 2019

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.
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[1] and under the Family Educational Rights and Privacy Act (FERPA).[2]
IV. Definitions	**Data:** • Expressed information representing facts in a variety of qualitative and quantitative forms, including aggregate, individual level, and personally identifiable information. **Data Files:** • Data files are physical and electronic representations of information, and any copies made. Examples of data files include but are not limited to: ○ Hard drives ○ Networking equipment ○ Paper printouts ○ Flash drives ○ Institutional servers ○ Any other type of materials that store, capture, or process data **Personally Identifiable Information (PII):** • PII is information that, alone or in combination with other data, can be linked to a specific student,[3] including but not limited to:[4] ○ Name of student, parents, or other family members; ○ Address of 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. **Data Sharing Agreement:** Data sharing agreements are legal documents between two or more parties that codify the terms and conditions for the sharing and use of data. OSSE requires agreements when sharing PII from education records with third parties.

[1]Privacy Technical Assistance Center, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282014-05-06%29%20%5BFinal%5D_0.pdf

[2] Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

[3] Any reference to "student" in this document intends to include any child, student or parent, as well as other individual-level records of others (such as teachers).

[4] Privacy Technical Assistance Center, http://ptac.ed.gov/glossary/personally-identifiable-informationeducation-records

	Data Destruction: • Data destruction is the process of removing information in a way that renders it unreadable (for paper records) or irretrievable (for digital records).[5] **De-identification:** • 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.[6] **Third Party:** • 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.
V. Policy	This policy sets requirements for documentation of data destruction plans and their completion by third parties under a written agreement. Third parties are not permitted to retain any data from OSSE beyond the terms of a data sharing agreement.[7] **There are no exceptions.** It is OSSE's policy not to enter into data sharing agreements without expiration dates. Under every data sharing agreement, the third party agrees to destroy all data shared: • 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. Third parties must submit a plan for data destruction for approval by OSSE. Once approved, the plan is incorporated into the written agreement. OSSE considers adherence to the Guidelines for Media Sanitization, issued by the National Institute of Standards and Technology (NIST),[8] to be compliant but will review and approve other plans on an individual basis. Third parties requesting such individualized plans must justify in writing why they cannot follow the NIST guidelines. OSSE does not consider third-party de-identification as data destruction. In cases where OSSE approves of another entity, such as another District of Columbia government agency, having access to de-identified student data because it serves a legitimate educational purpose, OSSE will require the agency to destroy the data originally provided and certify it has done so. OSSE will then provide a de-identified data set under a new written agreement. Third parties must document that they have destroyed all data files shared and how the data were destroyed.
VI. OSSE Expectations for Data Destruction	At the termination of an agreement, OSSE expects third parties to demonstrate that data destruction has rendered the data unreadable and/or irretrievable by submitting an OSSE-provided Certificate of Data Destruction. The certificate is required to be submitted within five

[5] Privacy Technical Assistance Center, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282014-05-06%29%20%5BFinal%5D_0.pdf

[6] US Department of Education, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/data_deidentification_terms_0.pdf

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

[8] https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

	days of the termination of the agreement and document compliance with the approved data destruction plan. The certificate must list all data files shared under the agreement and any copies made, with the third party indicating how each file was destroyed. Copies of files include anything residing in system backups, temporary files, or other storage media. Examples of destruction considered compliant include but are not limited to: • Clear, purge or destroy data files • Cross cut paper shredding • Hard disk physical destruction
VII. Monitoring Implementation	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.
VIII. 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.