Data Destruction Policy

CNMI PSS Data Governance Committee

REFERENCES:

Originator	*Data Governance Committee*
Effective Date	*June 11, 2025*
Approved by	*CNMI PSS Executive Leadership*
Statutory References	The Family Educational Rights and Privacy Act (FERPA) of 1974 (20 U.S.C. Sec. 1232g; 34 CFR Part 99) Individuals with Disabilities Education Act (34 CFR) Title 60-20: Retention of Records/Audit: §60-20-905 Retention of Records. CNMI regulation on retention for audit purposes. Title 60-30 Employment of Non-certified Personnel Regulation § 60-30.3-850 Record Retention and Reporting Requirements CNMI regulation on retention for Personnel. Title 60-40: Retention of Procurement Records: §60-40-270 Retention of Procurement Records. CNMI regulation for procurement-related record retention and destruction. Title 60-50: Destruction of Information: § 60-50-944 Destruction of Information. CNMI regulation on retention for SPED.

PURPOSE:

The purpose of this data destruction policy is to ensure that the CNMI Public School System (PSS) outdated or unnecessary data is securely and systematically destroyed to mitigate risks associated with data incidents, unauthorized access, and regulatory non-compliance. The retention and storage of outdated, unnecessary data, including data with expired retention periods, consumes valuable storage resources and increases the risk of data security incidents.

This policy establishes the requirements for identifying and safely disposing of data that is no longer necessary for operations, legal, or regulatory reasons while ensuring that longitudinal analysis needs are considered before disposal. Data identified for removal should be reviewed to ensure that essential longitudinal insights have been derived or preserved, supporting historical trend analysis and long-term outcome assessments.

SCOPE:
Applies to all individuals and groups involved in the handling, storage, and processing of CNMI PSS data. This includes employees and third parties who have access to CNMI PSS's data. The scope extends across all CNMI PSS data, whether physical or digital and all devices and systems where data is stored.

STATEMENT:
The **Data Destruction Policy** with the use of the **Data Destruction Assurance Form** establishes the principles and criteria to ensure the secure and proper disposal of data that has exceeded its defined retention period for school or program operations, legal compliance, or regulatory purposes. This policy applies to all types of data, regardless of format or storage location, and establishes clear rules and procedures for its destruction to protect privacy, reduce risks, and comply with applicable laws and Board of Education regulations. The **Data Destruction Assurance Form** ensures these principles are followed:

1. **Secure Data Disposal**:
    - Data no longer subject to statutory retention period for school or program operations, legal compliance, or regulatory purposes must be securely and permanently destroyed in accordance with this policy, while ensuring that longitudinal analysis needs (e.g., student performance, attendance records) are considered before disposal.
2. **Retention of Requested Records**:
    - Any educational record with an outstanding request to inspect and review that record will not be destroyed.
3. **Vendor and Contractor Obligations**:
    - All vendors, contractors, and external researchers must submit a completed Data Destruction Assurance Form.
    - All contracts will include provisions for vendor training to ensure they are aware of their obligations.
    - Vendors must submit a completed **Data Destruction Assurance Form**.
4. **Universal Applicability**:
    - This policy applies to all data formats (e.g., PDFs, spreadsheets, images, emails) regardless of storage location (e.g., cloud storage, local servers, physical archives).
5. **Legal and Regulatory Compliance**:
    - Data destruction methods must comply with all relevant legal standards (e.g., FERPA, COPPA), Board of Education regulations, all other applicable regulations, and best practices to ensure secure disposal.
6. **Oversight and Compliance Reviews**:

- All completed data destruction assurance forms are reviewed by the Data Governance Committee for compliance.

7. **Staff Protocol Adherence**:
    - All staff involved in data destruction must adhere to established protocols by the Data Governance Committee to ensure consistent, secure, and compliant disposal practices.

RESPONSIBILITIES:

1. **State Infrastructure Technology (SIT) Department**:
    - The SIT Department is tasked with executing the physical destruction of digital data across all systems, devices, and storage media. They are responsible for ensuring that all data destruction methods meet security standards and that procedures are followed properly.
    - Physically retrieve devices from departments or schools to wipe out digital data and ensure it is irretrievable.
    - Executing the degaussing or physical shredding of hard drives and other storage devices.
    - Creating a process to destroy digital data from assets assigned to employees who are no longer with PSS.
2. **Data Governance Committee**
    - The Data Governance Committee oversees the overall compliance with the Data Destruction Policy and the review of the **Data Destruction Assurance Form** submissions.
    - Ensure the timely submission and review of the **Data Destruction Assurance Form**.
    - Audit and verify that data destruction activities comply with the policy.
    - Provide guidance and updates on best practices for data management and destruction.
3. **Data Privacy Specialist**
    - The Data Privacy Specialist is responsible for reporting on compliance with the Data Destruction Policy to the Data Governance Committee
    - Provides training on the data destruction process
    - Report directly to the Data Governance Committee on compliance issues.
4. **Data Owners:**
    - Departments or individuals that manage highly confidential data, such as HR, Finance, Record Data Management (RDM), or Student Services, are responsible for classifying the data and ensuring it is properly flagged for destruction once its retention period has ended.

- Data identified for removal must be reviewed to ensure that essential longitudinal insights have been derived or preserved, supporting historical trend analysis and long-term outcome assessments.

5. **Third-Party (Vendors & Researchers)**:
    - Comply with handling of CNMI PSS data according to this policy.
    - Follow the data destruction protocols established in contracts or memorandum of understanding.
    - Provide evidence of secure destruction, such as certificates of destruction or the **Data Destruction Assurance Form,** when data destruction has been completed in reference to dates agreed to in the Data Destruction Assurance Form.
    - Notify CNMI PSS of any risks, breaches, or incidents related to data handling and destruction.
6. **All Employees**:
    - Every employee within CNMI PSS has a role in safeguarding data and ensuring it is properly destroyed when no longer needed.
7. **Executive Leadership**:
    - The executive leadership team, including department heads and school administrators, is responsible for overseeing the implementation of this policy across the organization
    - Ensure that all departments follow the Data Destruction Policy.
    - Allocate resources for training, auditing, and technology needed for secure data destruction.
    - Establish a culture of compliance and data security within their respective teams.

RELATED DOCUMENTS:

1. **Data Destruction Assurance Form**: CNMI PSS Data Destruction Assurance Form. Official form used to verify and document data destruction activities.
2. **Data Destruction Assurance Form Folder**: CNMI PSS Data Destruction Assurance Forms. Repository for completed assurance forms related to data destruction.
3. **Best Practices for Data Destruction (2019)**: Best Practices for Data Destruction (PDF). A U.S. Department of Education resource outlining secure data destruction methods and practices.
4. **Education and Office Record Retention Manual**: Manual for the Guidelines on Retention of Records.pdf. A guide detailing retention timelines and procedures for maintaining and disposing of records.
5. **Individuals with Disabilities Education Act (IDEA) §300.624 – Retention of Records**: 34 CFR §300.624. Federal regulation about record retention and destruction for individuals with disabilities.

6. **Individuals with Disabilities Education Act (IDEA) §300.611 – Definitions of Confidentiality and Destruction**: 34 CFR §300.611. Defines confidentiality and record destruction requirements under IDEA.

DEFINITIONS:

1. **Data Destruction**: The process of permanently erasing or eliminating data so that it is no longer accessible or recoverable by any means. This applies to both physical and electronic data.
2. **Data Owner**: The individual or department responsible for the maintenance, retention, and eventual destruction of specific datasets (e.g., HR for employee data, Finance for financial data).
3. **Digital Data**: Electronic records stored in databases, servers, cloud storage, or other digital platforms.
4. **Highly Confidential Data**: Information that, if breached, causes significant damage to PSS operations, reputation, and/or business continuity. Access to this information should be highly restricted. Student personally identifiable information (PII) falls into this category of data. Employee or Educator Financial Information, Social Security Numbers, and other critical information also fall into this classification.
5. **Personally Identifiable Information (PII)**: Any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. This may include names, Social Security numbers, dates of birth, and other data that could be used to identify an individual.
6. **Physical Data**: Any tangible records or documents, such as paper files or printouts, that contain information.
7. **Retention Period**: The legally or operationally required time that data must be stored before being destroyed. This varies depending on data type, regulatory requirements, and business needs.
8. **Third-Party**: External vendors, contractors, service providers, or researchers that store, process, or destroy data on behalf of CNMI PSS.

COMPLIANCE:

Adherence to this policy is mandatory. Compliance will be monitored through regular audits, continuous monitoring, self-assessments, and incident reporting. Enforcement actions for violations may include additional training.

TRAINING:
All employees, contractors, and third-party service providers will undergo mandatory training on data destruction. Refresher training will be conducted annually to reinforce and update knowledge.

COMMUNICATION:
This policy shall be distributed to all CNMI P12 Data Governance Committee members and personnel directly involved in the implementation. This policy will be stored electronically for access on the CNMI PSS or SLDS website and secured shared drive: P12 DGC Approved Policies.

REVISION HISTORY:

VERSION	DATE	DESCRIPTION OF CHANGE
1.0	5/13/2025	Initial Policy