CNMI PSS

COMMONWEALTH OF THE NORTHERN MARIANA ISLAN
PUBLIC SCHOOL SYST

CNMI Public School System

Educational and Office Record Destruction Standard Operation Procedure Manual

PSS Stadand Operation Procedure for Destruction of Physical and Digital Records

Executive Summary:

This executive summary outlines the best practice standard operating procedures (SOPs) for the destruction of physical and digital records in PSS (CNMI Public School System), as recommended by the PTAC (Privacy Technical Assistance Center). These procedures are designed to ensure compliance with data privacy and security regulations while effectively managing the destruction process for sensitive information.

I. Purpose:

The purpose of these SOPs is to provide PSS with a standardized and secure approach to the destruction of physical and digital records. By following these best practices, institutions can safeguard student and staff data, maintain regulatory compliance, and mitigate the risk of unauthorized access or data breaches.

II. Scope:

These SOPs apply to all physical and digital records maintained by PSS, including student records, employee records, financial documents, and any other confidential information collected and stored by the institution.

III. Records Inventory and Classification:

Institutions should conduct a thorough inventory of their records to identify and categorize them based on their sensitivity and confidentiality levels. This classification will help determine the appropriate destruction methods and retention periods for each type of record.

VI. Physical Record Destruction:

To destroy physical records, institutions should utilize secure methods such as shredding. Cross-cut or confetti shredders are recommended to ensure the effective destruction of confidential paper documents. Designated and locked disposal containers should be placed strategically throughout the institution and regularly emptied by authorized personnel.

V. Digital Record Destruction:

Digital records should be destroyed using secure methods to prevent unauthorized access or data recovery. Data wiping software or professional data destruction services should be employed to effectively erase data from storage devices. Magnetic media, such as hard drives or tapes, may be degaussed or physically destroyed to ensure complete data eradication.

VI. Compliance and Legal Considerations:

PSS must stay informed about applicable laws and regulations governing records destruction, including the Family Educational Rights and Privacy Act (FERPA) and other relevant data protection requirements. Compliance with data breach notification laws and other legal obligations should be ensured throughout the destruction process.

VII.Training and Awareness:

Proper training should be provided to staff members involved in the records destruction process. They should be educated on data privacy principles, records handling procedures, and the correct methods for destruction. Ongoing awareness programs should be implemented to promote a culture of data protection within the PSS.

VIII. Documentation and Audits:

Comprehensive documentation should be maintained throughout the destruction process, including destruction logs, certificates of destruction (if applicable), and any necessary notifications or approvals. Regular audits should be conducted to assess compliance with the records retention policy and the proper implementation of destruction procedures.

IX. Outsourcing:

In situations where resources or expertise may be lacking, PSSmay consider outsourcing the destruction of records to reputable third-party service providers. These providers should adhere to industry best practices and ensure the secure and compliant destruction of records.

X. SOP

By following these best practice SOPs for the destruction of physical and digital records,PSS can effectively protect sensitive information, meet regulatory requirements, and uphold their commitment to data privacy and security. Implementing these procedures will help mitigate the risk of unauthorized access or data breaches while maintaining compliance with relevant laws and regulations. According to PTAC, data related to students' transcript information may need to be preserved indefinitely. 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.

- Destruction of physical files
    - Contracts between PSS and vendors should include language assuring that the data was destroyed so that PSS is not held liable.
    - Records should be destroyed as soon as possible after the approved retention periods have lapsed.
    - After digitization, physical files will be destroyed after 5 years.
    - Shredders are considered the best, most effective way to completely destroy documents.
    - Destruction methods include burning, crosscut shredding, wet pulping, melting, mutilation, chemical decomposition, and pulverizing. Destruction methods must ensure that information is unrecoverable.
    - A log of records destroyed that meets the requirements of subsection must be kept for the destruction of records. The log should include a description of the records, the date range and amount of records, and the date, method and person responsible for destruction.
    - The individual who was responsible for destruction must complete and sign the Data Destruction Assurance form, which makes PSS no longer liable for the data.

- Destruction of digital files
    - Contracts between CNMI PSS and vendors should include language assuring that the digital data files were destroyed so that PSS is not held liable.
    - Digital records should be destroyed as soon as possible after the approved retention periods have lapsed.
    - A log of records destroyed that meets the requirements of subsection must be kept for the destruction of digital records. The log should include a description of the digital records, the date range and amount of records, and the date, method and person responsible for destruction.
    - The individual who was responsible for destruction must complete and sign the Data Destruction Assurance form, which makes PSS no longer liable for the data.

Methods of digital destruction

CLEAR - 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).

PURGE - A method of sanitization that applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.

DESTROY - 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.

PTAC's General Best Practices for Data Destruction:

- When drafting written agreements with third parties, include provisions that specify that all data that was provided to the third party must be destroyed when no longer needed for the specific purpose for which it was delivered, including any copies of the data that may reside in system backups, temporary files, or other storage media.
- Ensure accountability for the destruction of data by using certification forms signed by the authorized designee responsible for performing the destruction and containing detailed information about the destruction.
- Remember that data may also be present in non-electronic media. Organizations should similarly manage non-electronic records 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 shared data, be specific in the written agreement regarding 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. When a data file is often 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 the 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 ineffective because they leave most 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 promptly sanitization of storage media that 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.

DATA RISK CLASSIFICATIONS:

Low Risk

Data and systems are classified as Low Risk if they are not considered to be Moderate or High Risk, and:
1. The data is intended for public disclosure, or
2. The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our
mission, safety, finances, or reputation.

Moderate Risk

Data and systems are classified as Moderate Risk if they are not considered to be High Risk, and:
1. The data is not generally available to the public, or
2. The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on our mission, safety, finances, or reputation.

High Risk

Data and systems are classified as High Risk if:
1. Protection of the data is required by law/regulation,
2. PSS is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed, or
3. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact
on our mission, safety, finances, or reputation.

DATA CLASSIFICATIONS

Incidents vary in impact and risk depending on a number of mitigating factors including the content and quantity of the data involved. It is critically important that the PSS management responds quickly and identifies the data classification of the Incident. This allows staff to respond accordingly in a timely and thorough manner.

All reported Incidents shall be classified as below in order to assess risk and approaches to mitigate the situation. Data classification shall refer to the following PSS data categories:

Public Data - Information intended for public and community use or information that can be made

public without any negative impact on PSS or its stakeholders. Student PII shall never be considered public data unless the data is Directory Information as defined by Form 2420.1 (FERPA Notice of Designation of Directory Information) under Admin Code § 60-20-428.

Confidential/Internal Data - Information of a more sensitive nature to the business and educational operations of PSS. This data represents basic intellectual capital, applications, and general knowledge. Access shall be limited to only those people that need to know as part of their role within the PSS. Employee and Educator PII (with the exception of Social Security Numbers (SSN), financial information, or other critical information) falls within this classification.

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 PII falls into this category of data. Employee or Educator Financial Information, Social Security Numbers, and other critical information also fall into this classification.

NOTE: Reference Material used for Data Destruction SOP

(Below in Part A is wording from PTAC and Part B is the wording from Nora's CDI #12 Listing of Records Manual.
We can use this to prepare the SOP for Destruction of Records for CDI #13)

++++++++++++++++++++

PART A This is wording from PTAC Destruction of Records:
https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282019-3-26%29.pdf

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.CDI #13 - SOP for Destruction of Records

https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282019-3-26%29.pdf

++++++++++++++

PART B This is wording from Nora's CDI #12 Listing of Records Manual.

Records Retention and Disposition Schedule

The schedule in Appendix 1 provides minimum retention periods and dispositions for records commonly held by CNMI PSS school divisions/districts.

Some school divisions/districts may adopt the recommended retention periods. Others may decide to keep certain records longer than recommended, before destruction or archiving.

Records should **never** be destroyed sooner than recommended in the schedule in Appendix 1 because the school division/district may require this information for administrative, financial or legal purposes. Records designated as archival in the schedule in Appendix 1 should **never** be destroyed. The records management policy approved by the school board should include a schedule similar to that in Appendix 1, but it may be tailored as required for records held by the individual school division/district. The schedule should list records held by the school division/district and specify retention periods and dispositions.

- Destruction of physical files
    - Contracts between CNMI PSS and vendors should include language assuring that the data was destroyed so that PSS is not held liable.
    - Records should be destroyed as soon as possible after the approved retention periods have lapsed.
    - After digitization, physical files will be destroyed after 5 years.
    - Shredders are considered the best, most effective way to completely destroy documents.
    - Destruction methods include burning, crosscut shredding, wet pulping, melting, mutilation, chemical decomposition, and pulverizing. Destruction methods must ensure that information is unrecoverable.
    - A log of records destroyed that meets the requirements of subsection must be kept for the destruction of records. The log should include a description of the records, the date range and amount of records, and the date, method and person responsible for destruction.
    - The individual who was responsible for destruction must complete and sign the Data Destruction Assurance form, which makes PSS no longer liable for the data.
- Destruction of digital files
    - Contracts between CNMI PSS and vendors should include language assuring that the data was destroyed so that PSS is not held liable.
    - Records should be destroyed as soon as possible after the approved retention periods have lapsed.
    - A log of records destroyed that meets the requirements of subsection must be kept for the destruction of records. The log should include a description of the records, the date range and amount of records, and the date, method and person responsible for destruction.
    - The individual who was responsible for destruction must complete and sign the Data Destruction Assurance form, which makes PSS no longer liable for the data.