Data Privacy Policy

CNMI PSS Data Governance Committee

REFERENCES:

Originator	Data Governance Committee
Effective Date	June 11, 2025
Approved by	*CNMI PSS Executive Leadership*
Statutory Reference	• The Family Educational Rights and Privacy Act (FERPA) of 1974 (20 U.S.C. Sec. 1232g; 34 CFR Part 99) (https://www.ecfr.gov/current/title-34/subtitle-A/part-99) • Protection of Pupil Rights Amendment (PPRA) (34 CFR PART 98) • Admin Code Title 60: Board of Education (https://www.cnmilaw.org/admin.php#gsc.tab=0) • Individuals with Disabilities Education Act (IDEA) (https://www.ed.gov/laws-and-policy/individuals-disabilities/idea)

PURPOSE:

Data privacy is an essential aspect of the CNMI Public School System's (PSS) operations, ensuring the protection and responsible management of student and staff records, including Personally Identifiable Information (PII). The computer systems and devices used by CNMI PSS collect and process data necessary for educational delivery, administrative management, and reporting. Safeguarding this critical information from unauthorized access or disclosure is of paramount importance.

This policy outlines the specific conditions under which such information may be gathered, stored, and shared and requirements for managing information collected or generated through CNMI PSS operations, systems, network devices, and communications. It is designed to maintain the confidentiality and security of data while meeting the educational, operational, and compliance needs of the PSS.

SCOPE:

The Data Privacy Policy applies to school officials and stakeholders who create, deploy, or support the collection, processing, or management of CNMI PSS data wherein all types of data, including physical and digital records, student and staff information, and general network data are covered.

STATEMENT:

1. **Confidentiality**
    a. Student and staff Personally Identifiable Information (PII) collected by the CNMI Public School System (PSS) shall be kept confidential and protected from unauthorized access or disclosure.
2. **Data Collection**
    a. Student and staff data shall only be collected for legitimate educational, operational, or legal purposes as defined by local and federal laws.
3. **Data Disclosure**
    a. Student and staff data may only be shared with third parties when legally authorized or with the explicit consent of the PSS data owner.
    b. A written agreement must be established between the school official and the agency where the employee agrees to not disclose confidential information.
4. **Data Security**
    a. CNMI PSS will implement appropriate technical, administrative, and physical safeguards to protect all data from unauthorized access, alteration, or destruction.
5. **Data Integrity**
    a. To ensure data privacy, all information collected about students and staff must be accurate, complete, and up-to-date. Maintaining high data integrity ensures that decisions based on this data—such as educational planning, compliance reporting, or resource allocation—are made lawfully and ethically.
    b. Inaccurate or outdated data could lead to privacy violations, such as incorrect disclosures or misuses of personal information, thereby breaching privacy regulations and trust.
6. **Data Minimization**:
    a. As a core principle of data privacy, only the essential data needed to fulfill specific educational or administrative objectives should be collected, stored, or shared.
    b. Limiting data collection to what is strictly necessary reduces the risk of unauthorized access, accidental disclosure, or misuse of sensitive information.
7. **Access Control**
    a. Users should only have access to whatever confidential information necessary to perform tasks according to their roles, as outlined in the User Access Levels for Data Systems Policy.
8. **Data Retention & Destruction**:
    a. Student and staff records shall be retained only for as long as necessary to fulfill educational, legal, or compliance requirements, and securely disposed of when no longer needed.
    b. Data will be destroyed according to the Data Destruction policy.

9. **Data Transfer**:
    a. The transfer of student and staff data—whether within CNMI PSS offices or to authorized external entities—will be conducted in strict compliance with applicable data privacy laws and regulations.
    b. All data transfers must incorporate appropriate safeguards to protect the confidentiality, integrity, and security of personal information. This ensures that sensitive data is only shared with legitimate recipients for authorized purposes, minimizing the risk of unauthorized access, data breaches, or privacy violations.
10. **Data Breach Notification**
    a. In the event of a data breach, CNMI PSS will promptly notify affected individuals and relevant authorities in compliance with legal requirements, as stated in the CNMI PSS Data Breach Plan.
11. **Training and Awareness**:
    a. Comprehensive Data Privacy & Protection training is mandatory for all employees, contractors, non-employees, and third parties with access to CNMI PSS data.
    b. Role-specific training is required based on access levels.
    c. Training is required before access is initially granted and an annual refresher training is required thereafter to continue access.
    d. All training in the district should include a data privacy section.
12. **External Parties Compliance:**
    a. Vendors and contractors with access to CNMI PSS data must comply with all privacy and security policies.
    b. Formally signed agreements must detail the obligations for protecting data, conducting audits, notifying CNMI PSS of breaches or incidents, and destroying data after contract has expired, as outlined in the Data Destruction policy and any other applicable CNMI PSS data policies.
13. **Third-Party Compliance:**
    a. Non-employees, researchers, and service providers with access to CNMI PSS data must comply with all privacy and security policies.
    b. Formally signed agreements must detail the obligations for protecting data, conducting audits, notifying CNMI PSS of breaches or incidents, and destroying data after contract has expired, as outlined in the Data Destruction policy and any other applicable CNMI PSS data policies.

RESPONSIBILITIES:

1. **Data Governance Committee:**
    - Regularly review and update data privacy processes to remain compliant with changes in local, federal, and educational laws.
    - Establish a process for enforcing this Data Privacy Policy.

2. **Data Privacy Specialist:**
    - Oversee the implementation of and adherence to this policy. This includes ensuring adherence to legal and regulatory requirements for data collection, storage, sharing, and reporting, and addressing non-compliance.
3. **School Officials:**
    - Follow data privacy policies and procedures in their daily tasks. This includes handling student, staff, and operational data securely, reporting data breaches or suspicious activities, participating in mandatory training, and collaborating with other departments to ensure accurate and secure data sharing for operational purposes.
    - Responsible for maintaining the accuracy, quality, and security of data within their areas of control.
4. **Program Managers:**
    - Each program will be responsible for their data sharing agreement for internal and external data requests.
    - Program managers or designees will be responsible for ensuring that training for new and existing employees are conducted.
    - Responsible for ensuring that all applicable terms and conditions, contracts, or other data agreements prior to obtaining and/or procuring services or goods are reviewed and aligned with the CNMI PSS BOE Regulations, Policies, and other applicable local and federal laws.
5. **Procurement Office:**
    - Ensure that all vendor contracts adhere to data privacy and security policies, including the protection of sensitive data and adherence to applicable legal and regulatory standards.
6. **Office of State Infrastructure Technology (SIT)**:
    - Responsible for ensuring data security, network integrity, and protecting PII in digital systems when at rest and in transit.
7. **Human Resources (HR)**:
    - Responsible for managing employee information and following the data privacy policy regarding employee data.

RELATED DOCUMENTS:

1. Executive Data Governance Policy (2018) Executive DG Policy
2. CNMI PSS Breach Plan (2022) Data Breach Plan
3. User Access Levels for Data Systems Policy
4. Acceptable Use Regulation (2024) - www.cnmilaw.org
5. US Department of Education - Student Privacy Policy Office Training Modules:
    a. FERPA 101 Training: https://studentprivacy.ed.gov/training/ferpa-101-local-education-agencies

    b. FERPA 201 Training: https://studentprivacy.ed.gov/training/ferpa-201-data-sharing-under-ferpa
6. Privacy Technical Assistance Center (PTAC) https://studentprivacy.ed.gov/
7. All other related documents - published or drafted - will be uploaded to a designated section in the CNMI PSS District website - www.cnmipss.org

DEFINITIONS:

1. **Access Control:** The process of granting or restricting authorized users the ability to view, modify, or manage data within PSS-maintained systems, ensuring security and proper data governance.
2. **Confidentiality:** The state of keeping or being kept secret or private; confidentiality involves a set of rules or a promise sometimes executed through confidentiality agreements that limits the access to or places restrictions on the distribution of certain types of information.
3. **Data:** Encompasses all educational and personal information, including academic records, employee records, personal identifiers, behavioral data, and any other information collected, stored, or transmitted by the CNMI Public School System.
    a. **Student Information:** The PSS treats all student records as private and confidential. This data can only be obtained, stored, and used for legitimate educational purposes related to student achievement, accounting, pupil services, school operations, compliance, and audit purposes.
    b. **Staff Information:** This includes sensitive personal data related to staff of the CNMI PSS.
    c. **General Network Data:** Logs and other records capturing the use of the CNMI PSS systems and internet services and data used to ensure the proper functioning and security of the network.
4. **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).
5. **Data Privacy:** The protection of personal information from unauthorized access and ensuring that individuals have control over how their data is collected, used, shared, and stored.
6. **Data Protection:** The measures and practices that a school district must put in place to safeguard the privacy, confidentiality, and integrity of personal information collected, stored, or processed. This includes protecting data related to students, staff, and other stakeholders from unauthorized access, disclosure, or misuse.
7. **External Service Providers:** All vendors, contractors, and other service providers that handle, process, or access CNMI PSS data, including cloud services, data processors, and educational partners.

8. **FERPA:** The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."
9. **Formally Signed Agreements:** Includes, but not limited to, official contracts, terms and conditions, memorandum of understanding, and memorandum of agreement that has all required signatories.
10. **Non-employees:** Individuals who are not directly employed by the school district but may have access to its data, technology systems, or facilities as part of their roles (i.e. student teachers and interns). Non-employees are required to adhere to all applicable data privacy and security policies and are subject to the same confidentiality and data protection standards as employees.
11. **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.
12. **Students:** All students enrolled in the CNMI Public School System (PSS), their parents or guardians, and eligible students, as defined by FERPA, have rights regarding their education records under the Family Educational Rights and Privacy Act (FERPA).
13. **School Officials:** Any employee, including teacher, that the school or district has determined to have a "legitimate educational interest" in the personally identifiable information from an education record of a student. School officials may also include third party contractors, consultants, volunteers, service providers, or other parties with whom the school or district has outsourced institutional services or functions for which the school or district would otherwise use employees under the school official exception in FERPA.
14. **Third-Parties:** Includes authorized government agencies, researchers, and other entities with whom data may be shared in compliance with legal obligations or under explicit consent.

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 privacy. 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