

INTERNAL DATA SHARING AGREEMENT

This Internal Data Sharing Agreement (“Internal DSA”) is entered into by the CNMI State Longitudinal Data System (“CNMI SLDS”), whose address is P.O. Box 501370 CK, Saipan, MP 96950, and the CNMI Public School System’s Department/Program/Office (herein called the “PSS Data Provider”). The purpose of this Internal DSA is to acknowledge the conditions for which data will be linked and analyzed in the SLDS. The effective date of this Internal DSA shall be the date of the last signature of the parties affixed to this Internal DSA.

I. PURPOSE

The CNMI SLDS and PSS Data Provider have agreed to: coordinate and share data to develop a longitudinal data system for the CNMI Public School System, (SLDS Goal 1) and support objective analysis and reliable conclusions based on longitudinal education data (SLDS Goal 2). These are also in support of achieving the CNMI Public School System’s Vision and Mission:

- Vision: The Commonwealth of the Northern Mariana Islands Public School System is a provider of quality education, empowering all individuals to be innovative thinkers and learners.
- Mission: Educating lifelong learners to become productive citizens of a global society.

To achieve the goals of this Internal DSA, it is necessary for the PSS Data Provider to share the specific Data Elements Listing provided in Appendix B to verify student status, evaluate and analyze students’ respective educational and program information to improve student performance outcomes, and to enforce or comply with federal and local legal requirements that relate to federal and state programs supported by CNMI SLDS. The PSS Data Provider agrees that any shared data shall be used for evaluation purposes to assess the impact and improvement of instruction, programs, and educational and early intervention services.

In compliance with the Family Educational Rights and Privacy Act (“FERPA”) (20 U.S.C. 1232g and 34 CFR Part 99) sections 99.31(a)(1)(i)(B), CNMI PSS designates DBDriven as its “School Official”. FERPA (§ 99.31(a)(1)(i)(B)) permits schools to outsource institutional services or functions that involve the disclosure of education records to contractors, consultants, volunteers, or other third parties provided that the outside party:

- Performs an institutional service or function for which the agency or institution would otherwise use employees;
- Is under the direct control of the CNMI PSS with respect to the use and maintenance of education records;
- Is subject to the requirements in § 99.33(a) that the personally identifiable information (PII) from education records may be used only for the purposes for which the disclosure was made, e.g., to promote school safety and the physical

security of students, and governing the redisclosure of PII from education records; and

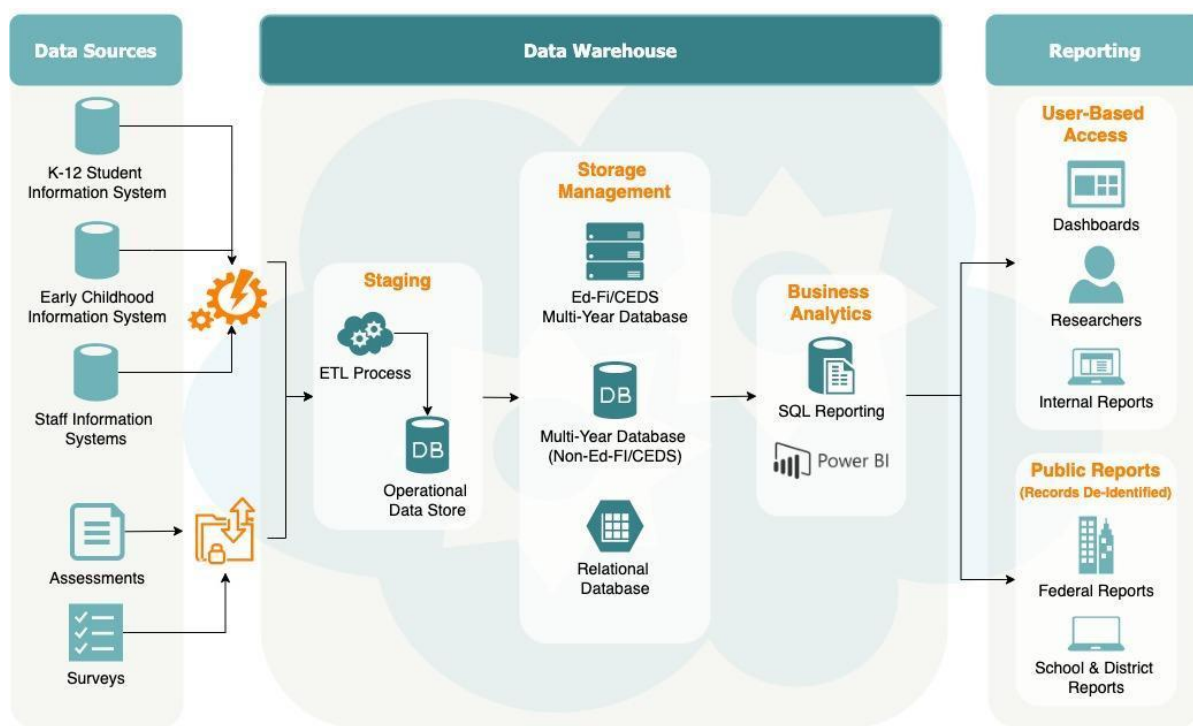
- Meets the criteria specified in the CNMI PSS annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records.

II. LEGAL AUTHORITY/JUSTIFICATION

CNMI Board of Education's regulation on Student Records, and in compliance with all applicable federal and CNMI laws and regulations that protect student information, the Party shall comply in all respects reasonably pertinent to this agreement with the provision of FERPA. For purposes of this Internal DSA, "FERPA" includes any amendments or other relevant provisions of federal law, as well as all requirements of Chapter 99 of Title 34 of the Code of Federal Regulations. Nothing in this Internal DSA may be construed to allow either party to maintain, use, disclose or share student information in a manner not allowed by federal law or regulation.

III. SLDS DATA WAREHOUSE INFRASTRUCTURE

The high-level architecture diagram below shows the flow of data from data sources (by the data stewards) through the Data Warehouse to the reports and dashboards.



IV. TERMS AND CONDITIONS

To affect the transfer of data subject to FERPA, the PSS Data Provider agrees to the following provisions:

1. Definition of Data. Data includes all Personally Identifiable Information (PII) and other non-public information. Data include, but are not limited to, student data, metadata, and user content.
2. Data Quality Measures. A data quality involves measuring data based on a characteristic, aspect, or feature that provides a way to classify information and data quality needs. Managing data quality ensures a unified approach to data entry, thus ensuring greater validity of data at the source of the data lifecycle. The Data Provider agrees to the following data quality measures:
 - a. **Accurate:** Values reflect the data element definition and correctly capture the “real life” object it intended to model.
 - b. **Complete:** All required fields contain values.
 - c. **Consistent:** The same data across the organization are in sync with one another and over time.
 - d. **Relevant:** The definition and business rules are aligned with the intended use(s).
 - e. **Timely:** The data are collected and available when needed to fulfill their intended uses.
 - f. **Trusted:** Data users believe that the data are of sufficient quality and appropriate for the intended use(s).
 - g. **Secure:** Data is protected from unauthorized access, corruption, and destruction.
 - h. **Accessibility:** Authorized users can readily view and retrieve the data they need, in the form they need it.
 - i. **Validity:** The measurements reflect what they are supposed to measure.
3. Data De-Identification. The CNMI SLDS may use de-identified data for product development, research, or other purposes. De-identified data will have all direct and indirect personal identifiers removed. This includes, but is not limited to, name, ID numbers, date of birth, demographic information, location information, and school ID. Furthermore, the CNMI SLDS agrees not to attempt to re-identify de-identified data and not to transfer de-identified data to any party unless that party agrees not to attempt re-identification.
4. Marketing and Advertising. Data may not be used for any purpose other than the specific purpose(s) outlined in this Agreement. The CNMI SLDS will not use any data to advertise or market to students or their parents. Advertising or marketing may be directed to the PSS Data Provider only if student information is properly de-identified.
5. Modification of Terms of Service. The CNMI SLDS will not change how data is collected, used, or shared under the terms of this Agreement in any way without advance notice to and consent from the appropriate PSS Data Provider.
6. Data Collection. The CNMI SLDS will only collect data necessary to fulfill its duties as outlined in this Agreement.
7. Data Use. The CNMI SLDS will use data only for the purpose of fulfilling its duties and providing services under this Agreement, and for improving services under this Agreement.

8. Data Mining. The CNMI SLDS is prohibited from mining data for any purposes other than those agreed to by the parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited.
9. Data Sharing. The PSS Data Provider understands that the CNMI SLDS will rely on one or more subcontractors to perform services under this Agreement. The CNMI SLDS agrees to share the names of these subcontractors with User upon request. All subcontractors and successor entities of the CNMI SLDS will be subject to the terms of this Agreement. Subcontractors will not disclose the information to any other party without the prior consent of the parent/guardian or eligible student. Each party to whom disclosure may be made under this agreement must first sign a statement in which he/she/it agrees to abide by this provision and agrees to use the information disclosed only for the purposes for which the disclosure was made.
10. Data Transfer or Destruction. The CNMI SLDS will ensure that all data in its possession and in the possession of any subcontractors, or agents to which the CNMI SLDS may have transferred data, are destroyed or transferred to the PSS Data Provider under the direction of the PSS Data Provider when the data are no longer needed for their specified purpose at the request of the PSS Data Provider.
11. Rights and License in and to Data. Parties agree that all rights, including all intellectual property rights, shall remain the exclusive property of the PSS Data Provider, and the CNMI SLDS has a limited, nonexclusive license solely for the purpose of performing its obligations as outlined in the Agreement. This Agreement does not give the CNMI SLDS any rights, implied or otherwise, to data, content, or intellectual property, except as expressly stated in the Agreement. This includes the right to sell or trade data.
12. Access. Any data held by the CNMI SLDS will be made available to the PSS Data Provider upon request by the PSS Data Provider.
13. Security Controls. The CNMI SLDS will store and process data in accordance with industry best practices. This includes appropriate administrative, physical, and technical safeguards to secure data from unauthorized access, disclosure, and use. The CNMI SLDS will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. The CNMI SLDS will also have a written incident response plan, to include prompt notification of the affected PSS Data Provider in the event of a security or privacy incident, as well as best practices for responding to a breach of PII. The CNMI SLDS agrees to share its incident response plan upon request.
14. Breach and Default. Upon breach or default of any of the provisions, obligations, or duties embodied in this agreement, the parties may exercise any administrative, contractual, equitable, or legal remedies available, without limitation. The waiver of any occurrence of breach or default is not a waiver of such subsequent occurrences, and the parties retain the right to exercise all remedies mentioned herein.

15. Annual Review of this Internal DSA. This shall be reviewed on an annual basis to ensure adherence to federal, local and partner internal policies regarding sharing of confidential data. The CNMI SLDS Director or designee shall decide if changes to the Internal DSA may be handled by amendment to this Internal DSA.
16. Signatures in counterpart. This Internal DSA may be executed in counterparts, each of which shall be deemed an original, and the counterparts together shall constitute one and the same Internal DSA. Duplicate, unexecuted pages of the counterparts may be discarded and the remaining pages assembled as one document for all purposes, including recordation, filing and delivery of this Internal DSA. The submission of a signature page transmitted by facsimile or similar electronic transmission facility shall be considered to be an original signature page for the purposes of this Internal DSA.

V. SIGNATURES

We have reviewed and hereby agree to abide by the data transfer agreement, as authorized by the Designated Authorities and Data Transfer requirements in Appendix A; the authorized Data Elements Listing in Appendix B and Vendor-to-Vendor Data Sharing Agreement in Appendix C:

CNMI SLDS

SLDS Project Director (or Designee):

Name _____ Signature _____ Date _____

PSS DATA PROVIDER

Data Steward

Name _____ Signature _____ Date _____

Supervisor

Name _____ Signature _____ Date _____

Appendix A. Designated Authorities and Transfer Requirements

Appendix B. Data Elements Listing

Appendix C. Vendor-to-Vendor Sharing Agreements

- ☐ Data Sharing Agreement is attached
- ☐ Not Applicable