DATA SHARING AGREEMENT BETWEEN
THE CNMI PUBLIC SCHOOL SYSTEM AND
Northern Marianas Technical Institute
TO SUPPORT THE P-20W DATA GOVERNANCE PROGRAM

I. INTRODUCTION

This Data Sharing Agreement ("DSA") is entered into by and between the CNMI Public School System (PSS) and the CNMI Department of Finance (hereinafter referred to as the "Partner Agency") to facilitate the CNMI Statewide Longitudinal Data System (SLDS). The CNMI SLDS brings together cross-agency, longitudinal data from preK-12 and postsecondary education into the workforce. The effective date of this DSA shall be the date of the last signature of the parties to this DSA affixed to this DSA. (Refer to Appendix A for Designated Authorities and Data Transfer Requirements)

II. PURPOSE

The purpose of this DSA is to formalize the collaboration between PSS and the Partner Agency in sharing individual-level data to support the objectives of the CNMI SLDS. It operationalizes the commitments established in the MOU by defining the procedures, responsibilities, and protections required for interagency data exchange under the CNMI P20W Data Governance Program.

This collaboration is based on a six-partner memorandum of understanding ("MOU") signed by the CNMI Department of Commerce ("DOC"), CNMI Department of Finance ("DOF"), CNMI Department of Labor ("DOL"), CNMI Public School System (PSS), Northern Marianas College ("NMC"), and Northern Marianas Technical Institute ("NMTech"), which was implemented in March 2024. The Partners recognize that each Partner Agency contributes to the progression of students through the education to workforce pipeline. Data collected by the Partners Agency provides information to ensure the quality, integrity, and accessibility of data for informed decision-making, accountability, and continuous improvement across our educational and workforce ecosystem. This DSA ensures responsible data use through a secure framework that supports research, compliance, and system-wide improvement.

III. SCOPE

This DSA governs the privacy and security conditions for the collection, storage, processing, use, and sharing of data pertaining to individuals' educational and workforce records, including Personally Identifiable Information (PII). It applies to all data exchanged between PSS and the Partner Agency within the framework of the P20W Data Governance Program; In the event of a

conflict between this DSA and P20W Data Governance policies, this DSA shall control only

with respect to the rights and obligations of the Parties to this Agreement, provided that such provisions remain compliant with FERPA and applicable CNMI laws.”however, if the content of a Data Governance policy or process conflicts with the DSA, the DSA supersedes it. The Parties agree to adhere to the terms and conditions outlined herein to ensure the responsible and secure handling of data throughout its lifecycle. (Refer to Appendix B for the Authorized Data Elements Listing).

Shared data contributed by the Partners is stored within eMPowerED, which is the CNMI SLDS data warehouse. The P20W Data Governance will create data policies and processes that will define how data will be managed throughout the information lifecycle in support of the program’s purpose.

IV. LEGAL AUTHORITY/JUSTIFICATION

All procedures and systems developed and implemented to process, store, or transmit data under this Data Sharing Agreement (DSA) shall uphold the privacy and confidentiality rights of individuals in full compliance with applicable federal and CNMI laws and policies. P20W Data Governance policies shall align with, but are not limited to, the Family Educational Rights and Privacy Act (FERPA) of 1984 (20 U.S.C. § 1232g; 34 CFR Part 99), the National School Lunch Act (42 U.S.C. § 1788; 7 CFR § 245.6), the Internal Revenue Code of 1954 (26 U.S.C. § 6103; 26 CFR), the CNMI Statistical Act of 1990 (Public Law 7-35), the Education Act of 2017 (3 CMC §§ 1101–1172), and the Postsecondary Education Act of 1984 (Public Law 4-34). It also observes statutory mandates related to the establishment of key public institutions, including 1 CMC §§ 2251, 2451, 2551, and 2831, as well as 3 CMC §§ 1304 and 12104.

The CNMI Public School System (PSS), as a state educational authority under 34 C.F.R. § 99.31(a)(3)(iv), is authorized by federal and CNMI laws to access education records to perform audits, evaluations, and compliance activities as defined in 34 C.F.R § 99.35(a).

Partner Agencies may access education records under this DSA only to the extent permitted by applicable law, including FERPA §99.31(a)(3) (authorized representative for audit/evaluation) and §99.31(a)(6) (studies exception), and must execute this DSA as a condition of access.Partner

Furthermore, education records provided for inclusion in the CNMI SLDS under 34 C.F.R. § 99.31(a)(6)(i) enable educators and policymakers to derive deeper insights, thereby fostering informed decision-making that promotes educational advancement across all levels.

V. Definitions

A. Data: Data includes all Personally Identifiable Information (PII) and other non-public information. Data includes, but is not limited to, student data, workforce data, and user content.

B. Data Quality Standards: Data quality standards are metrics used to assess a characteristic, aspect, or feature 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. It allows organizations to ensure that their data is reliable and suitable for its intended use. Each Partner Agency agrees to designate appropriate personnel and resources to ensure compliance with these the following data quality standards:

    1. Accurate: Values reflect the data element definition and correctly capture the "real life" object it intended to model. It assesses whether the data is free from errors or mistakes.
    2. Complete: All required fields contain values. This measures whether all required data is present. It ensures that there are no missing values in the dataset.
    3. Consistent: The same data across the organization are in sync with one another and over time. It checks whether the data is free from contradictions or discrepancies.
    4. Relevant: Measures the usefulness of data for its intended purpose. It assesses whether the data aligns with the needs and objectives of the organization.
    5. Timely: Measures how up-to-date the data is. It evaluates whether the data is available within an acceptable timeframe for its intended use.
    6. Trusted: Data users believe that the data are of sufficient quality and appropriate for the intended use(s). It checks whether the data is free from contradictions or discrepancies.
    7. Secure: Data is protected from unauthorized access, corruption, and destruction.
    8. Accessible: Authorized users can readily view and retrieve the data they need, in the form they need it.
    9. Validity: Measures the conformity of data to predefined rules or standards. It checks whether the data meets the specified criteria or requirements.

C. Processing: Any operation or set of operations performed on data, whether or not by automated means, including but not limited to collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.

VI. TERMS AND CONDITIONS

NOW, THEREFORE, the Partner Agency providing data agrees to the following:

1. Authority: PSS is granted authority to receive data from Partner Agency and other contributing CNMI agencies for the purpose of creating and maintaining the CNMI SLDS, which requires data sharing agreements for all access to SLDS data.

2. Access: Any data held by the PSS will be made available to the Partner Agency upon request by the Partner Agency.

3. Rights and License in and to Data: Parties agree that all rights, including all intellectual property rights, shall remain the exclusive property of the Partner Agency, and the PSS has a limited, nonexclusive license solely for the purpose of performing its obligations as outlined in the DSA. This DSA does not give the PSS any rights, implied or otherwise, to data, content, or intellectual property, except as expressly stated in the DSA. This includes the right to sell or trade data.

4. Data Collection: PSS will only collect data necessary to fulfill responsibilities as outlined in this DSA. Specific data elements collected under this Agreement are detailed in Appendix B.

5. Data Use: PSS will use data only for the purpose of fulfilling responsibilities and providing services to Partner Agencies under this DSA, and for improving services under this DSA.

6. Data De-Identification: PSS 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, PSS 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. Identifiable data, including records containing small cell sizes or unsuppressed results, may be used by Partner Agencies strictly for internal program improvement, monitoring, and compliance activities, consistent with their authority under 34 CFR § 99.35.

7. Data Mining: PSS 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 is prohibited.

8. Marketing and Advertising: Data may not be used unless aligned with the purpose referenced in page 1 of this DSA. PSS will not use any data to advertise or market to students or their parents. Advertising or marketing may be directed to the Partner Agency only if information is properly de-identified and such use is strictly limited to internal agency awareness or communication purposes. De-identified data shall not be used for public-facing or commercial messaging, nor shall it be re-identified or combined with other datasets to infer individual identity.

9. Data Sharing: The Partner Agency acknowledges that all contractors or third-party vendors engaged by PSS to access SLDS data must sign a written agreement that meets the requirements of 34 CFR §99.31(a)(3)(iii) or (a)(6)(iii), including data destruction, purpose limitation, and prohibition on redisclosure. These contractors may access, use, and maintain data solely for purposes aligned with the SLDS, and their identities shall be made available to the Partner Agency upon request. While contractors are not parties to this DSA, PSS shall ensure that they are bound by separate written agreements—referenced in Appendix C—that impose obligations consistent with the privacy, security, and data governance standards established in this DSA. Access to data shall be restricted to individuals with direct SLDS-related responsibilities, who must complete data privacy and security training and remain under appropriate supervision. Data may not be used, duplicated, or disclosed by contractors for any purpose beyond the scope of their contractual obligations without prior written consent from PSS and the Partner Agency.

10. Data Transfer or Destruction: PSS will ensure that all data in its possession and in the possession of any subcontractors, or agents to which PSS may have transferred data, are destroyed or transferred to the Partner Agency under the direction of the Partner Agency when the data are no longer needed for their specified purpose at the request of the Partner Agency.

11. Security Controls: PSS will store and process data in accordance with industry best practices. This process includes appropriate administrative, physical, and technical safeguards to secure data from unauthorized access, disclosure, and use. PSS will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. PSS will also have a written incident response plan, to include prompt notification of the affected Partner Agency in the event of a security or privacy incident, as well as best practices for responding to a breach of PII. PSS agrees to share its incident response plan with all Partner Agencies involved in data sharing.

12. Data Breach Notification Protocol: In the event of a data breach, PSS shall promptly notify the Partner Agency, adhering to established timelines as outlined in the incident

response plan. Notification will include comprehensive details of the breach, actions taken for resolution, and preventive measures to mitigate future occurrences.

13. Modification of Terms of Service: PSS will not change how data is collected, used, or shared under the terms of this DSA in any way without advance notice to and consent from the Partner Agency.

14. Annual Review of this DSA: PSS shall have the discretion to review this DSA at least once every three (3) years 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 DSA may be handled by amendment to this DSA.

15. Dispute Resolution: In cases of disagreement or dispute arising from this agreement, the parties shall engage in good faith negotiations to resolve issues amicably. If the Parties are unable to resolve the dispute through negotiation within 30 days, either Party may pursue administrative remedies pursuant to the CNMI Administrative Procedures Act. The Parties certify that all data exchanges under this DSA are conducted in accordance with FERPA and applicable CNMI privacy laws, and that access is granted only to individuals with a legitimate educational interest, or as permitted under the audit/evaluation or studies exceptions at 34 CFR §§ 99.31 and 99.35.

16. Indemnification and Hold Harmless: It is understood that the CNMI SLDS Program, its Executive Leadership, the CNMI Public School System (PSS), and the Partner Agency are joined for the purpose of this Data Sharing Agreement to support the secure and lawful exchange of data under the P20W Data Governance Program. Each Party agrees to indemnify, defend, and hold harmless the other Party and its respective officers, directors, employees, and agents from and against any and all third-party claims, actions, liabilities, losses, damages, expenses, and costs (including, but not limited to, reasonable attorneys' fees) arising out of or related to the data sharing activities performed under this Agreement, except to the extent such claims result from the willful misconduct or gross negligence of the indemnified Party. This clause shall survive the termination or expiration of this Agreement.

17. 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.

18. Signatures in counterpart: This DSA may be executed in counterparts, each of which shall be deemed an original, and the counterparts together shall constitute one and the same 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 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 DSA.

19. The Memorandum of Understanding (MOU) entered into by the CNMI Department of Commerce, Department of Finance, Department of Labor, Northern Marianas College, Northern Marianas Technical Institute, and the CNMI Public School System shall be incorporated into the current Data Sharing Agreement (DSA). The terms and conditions of the MOU are hereby referenced and incorporated herein and are binding on all parties. In the event of any conflict between the DSA and the MOU, the terms of the MOU shall govern. If any provision is included in the MOU but not in the DSA, such omission is intentional, and the absence of a provision in the DSA shall not be construed as limiting its applicability or enforceability.

IV. 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 the Vendor's Data Sharing Agreement in Appendix C:

CNMI SLDS

SLDS Project Director (or Designee):

Name: Annette Pladevega Sablan, SLDS Project Director

Signature _____ Date: September 11, 2025

PARTNER AGENCY

Northern Marianas Technical Institute - P20W Executive Leadership

Name: Jodina Attao, CEO

Signature _____ Date 10/2/2025

Appendix A. Designated Authorities and Data Transfer Requirements

NMTech - Designated Authorities and Data Transfer Requirements	
Data Source	From 2021 Fall to 2023 Spring will be on a spreadsheet. From 2023 Fall and forward, will be on our database application Class 365
Data Steward	Leo Master (leo.master@nmtechcnmi.org)
Vendor Company Name	CD Consulting
Vendor POC Information	Dan Camacho 670-483-3264
Location of Data (on-prem, cloud)	Cloud
Earliest Year	2021 Fall on Spreedsheet & 2023 Fall on DB App
Last Year	2025 Spring
Target Refresh Rate for Data Source (e.g. daily, weekly, quarterly, etc)	Daily
Data Acuisition Type (API, Portal Download, etc)	Portal
Requirements Gathered	
File download/extract format (.csv)	.csv
Is the system being replaced, if please provide ETA and new system if available	No

Appendix B. Data Elements Listing

Valid Value	Description	Data Classification	Rationale	Security Control
Student No.	Student ID number generated once fully enrolled via online portal	Internal	Relevant to NMTech only	3 - Low
NCCER No.	Designated NCCER number given when reigstered into NCCER website / database	Confidential	Required by NCCER registrar to verify certifications and qualifications	2 - Moderate
Cycle Applied For	Indicates which semester / cohort student is currently enrolled within school year	Internal	Relevant to NMTech only	4 - Open
Status	Indicates whether student is Ongoing / New / Returning	Internal	Relevant to NMTech only	4 - Open
Trade	Current Trade enrolled into	Internal	Relevant to NMTech only	3 - Low
Last Name	Student Legal Last Name	Confidential	Student Personal Information	2 - Moderate
First Name	Student Legal First Name	Confidential	Student Personal Information	2 - Moderate
Middle Name	Legal Middle Name (if applicable)	Confidential	Student Personal Information	2 - Moderate
Date of Birth	Student Birth Month / Day / Year	Confidential	Student Personal Information	2 - Moderate
Age	Current Age	Internal	Student Personal Information	3 - Low
Gender	Gender Identity	Internal	Student Personal Information	3 - Low
Student Contact Information	Contact Numbers; Home & Cellphone	Confidential	Student Personal Information	1 - High
Email Address	Student Valid Email	Confidential	Student Personal Information	1 - High
Mailing Address	Student P.O Box Address	Confidential	Student Personal Information	2 - Moderate
City	City Student Reside In	Internal	Student Personal Information	3 - Low
State	State Of the City Student Resides In	Internal	Student Personal	3 - Low

			Information	
Zip Code	ZIP code of State the Student Resides In	Internal	Student Personal Information	4 - Open
Village	Name of Village Student Resides In	Internal	Student Personal Information	3 - Low
Citizenship	Student's Birth Citizenship	Internal	Student Personal Information	4 - Open
Race/Ethnicity	Ancestry and/or Cultural Identity	Internal	Student Personal Information	4 - Open
Court Records	Indication if Student has any criminal court record we should be aware of (current or past)	Confidential	Student Personal Information	2 - Moderate
Educational Background	Highest Level of Education Acheived (if applicable)	Internal	Student Personal Information	3 - Low

Appendix C. Vendor's Data Sharing Agreements