

---

### MOORE PUBLIC SCHOOLS DATA PRIVACY MEMORANDUM OF AGREEMENT

Executed and effective as of the 15th day of May, 2022, by and

between NCS Pearson, Inc., (the "Company"),

and Moore Public Schools (**MOORE**), a public school system organized and existing under the laws of the state of Oklahoma (the "School Board"), recites and provides as follows.

#### Recitals

The Company and the School Board are parties to a certain agreement entitled hereafter referred to as (the "Agreement"). In connection with the execution and delivery of the Agreement, the parties wish to make this Memorandum of Agreement (also referred to as MOA or Addendum) a part of the original Agreement in order to clarify and/or make certain modifications to the terms and conditions set forth in the original Agreement.

The Company and the School Board agree that the purpose of such terms and conditions is to ensure compliance with the Family Educational Rights and Privacy Act (FERPA) and the overall privacy and security of student and staff Personally Identifiable Information (PII) hereafter referred to as student/staff information and/or data, including but not limited to (a) the identification of the Company as an entity acting for the School Board in its performance of functions that a School Board employee otherwise would perform; and (b) the establishment of procedures for the protection of PII, including procedures regarding security and security breaches.

**NOW, THEREFORE**, for good and valuable consideration, the receipt and sufficiency of which is acknowledged hereby, the parties agree as follows.

#### Agreement

The following provisions shall be deemed to be include but limited to:

- Student/Staff data storage, maintenance, collection, integration, and/or analysis
- Special Education consultation, audit, evaluation, behavior intervention supports
- Academic consultation, audit, evaluation, behavior intervention supports
- Information technology maintenance, integration, consultation or audits

**Confidentiality Obligations Applicable to Certain Moore Student Records.** The Company hereby agrees that it shall maintain, in strict confidence and trust, all Moore student records containing personally identifiable information (PII) hereafter referred to as "Student Information". Student information will not be shared with any other resource or entity that is outside the intended purpose of the Agreement.

**Data Checklist (Attachment 1) must completed and submitted to identify all data used by the vendor for public record.**

The Company shall cause each officer, director, employee and other representative who shall have access to Moore Student Records during the term of the Agreement (collectively, the "Authorized Representatives") to maintain in strict confidence and trust all Moore Student Information. The Company shall take all reasonable steps to insure that no Moore Student or Staff information is disclosed to any person or entity except those who (a) are Authorized Representatives of the Company performing functions for Moore under the Agreement and have agreed to be bound by the terms of this Agreement; (b) are authorized representatives of Moore, or (c) are entitled to such Moore student information from the Company pursuant to federal and/or Oklahoma law. The Company shall use Moore's data, and shall take all reasonable steps necessary to ensure that its Authorized

Representatives shall use such information, solely for purposes related to and in fulfillment of the performance by the Company of its obligations pursuant to the Agreement.

The Company shall: (a) designate one of its Authorized Representatives to be responsible for ensuring that the Company and its Authorized Representatives maintain the Moore student information as confidential; (b) train the other Authorized Representatives with regard to their confidentiality responsibilities hereunder and pursuant to federal and Oklahoma law; (c) maintain at all times a list of Authorized Representatives with access to Moore student information.

**Other Security Requirements.** The Company shall maintain those technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of Moore student information, including procedures to (a) establish user IDs and passwords as necessary to protect such information; (b) protect all such user passwords from detection and unauthorized use; (c) prevent hostile or unauthorized intrusion that could result in data corruption, or deny service; (d) prevent and detect computer viruses from spreading to disks, attachments to e-mail, downloaded files, and documents generated by word processing and spreadsheet programs; (e) minimize system downtime; (f) notify Moore of planned system changes that may impact the security of Moore data; (g) return or destroy Moore data that exceed specified retention schedules; (h) notify Moore of any data storage outside the US, Canada or Ireland; (i) in the event of system failure, enable immediate recovery of Moore information to the previous business day. The Company should guarantee that Moore data will not be sold to, accessed by, or moved by third parties.

In the event of a security breach, the Company shall (a) immediately take action to close the breach; (b) notify Moore within 5 working days of Company's first knowledge of the breach, the reasons for or cause of the breach, actions taken to close the breach, and identify the Moore student information compromised by the breach; (c) return compromised Moore data for review; (d) provide communications on the breach to be shared with affected parties and cooperate with Moore's efforts to communicate to affected parties by providing Moore with prior review of press releases and any communications to be sent to affected parties; (e) take all legally required, reasonable, and customary measures in working with Moore to remediate the breach which may include reimbursing Moore for the reasonable expenses incurred by Moore to provide upon to three (3) months of toll free telephone support with informed customer services staff to address questions by affected parties, and/or providing upon to one (1) year of credit-monitoring services for affected parties; (f) cooperate with Moore by providing information, records and witnesses needed to respond to any government investigation into the disclosure of such records or litigation concerning the breach; and (g) provide Moore with notice within 5 working days of notice or service on Company, whichever occurs first, of any lawsuits resulting from, or government investigations of, the Company's handling of Moore data of any kind, failure to follow security requirements and/or failure to safeguard Moore's data. The Company's compliance with the standards of this provision is subject to verification by Moore personnel or its agent at any time during the term of the Agreement. Said information should only be used for the purposes intended and shall not be shared, sold, or moved to other companies or organizations nor should other companies or organization be allowed access to said information.

### **Disposition of Moore Data upon Termination of Agreement**

Upon expiration of the term of the Agreement, or upon the earlier termination of the Agreement for any reason, the Company agrees that it promptly shall deliver to the School Board, and shall take all reasonable steps necessary to cause each of its Authorized Representatives promptly to deliver to the School Board, all required Moore student data and/or staff data. **See Attachment 2: Disposition of Data.** The Company hereby acknowledges and agrees that, solely for purposes of receiving access to Moore data and of fulfilling its obligations pursuant to this provision and for no other purpose (including without limitation, entitlement to compensation and other employee benefits), the Company and its Authorized Representatives shall be deemed to be school officials of the School Board, and shall maintain Moore data in accordance with all federal state and local laws, rules and

# Center for Technology

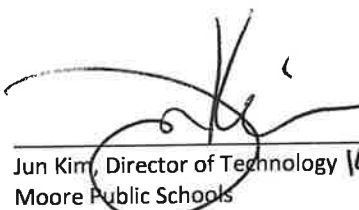
## Memorandum of Agreement (MOA)

regulations regarding the confidentiality of such records. The non-disclosure obligations of the Company and its Authorized Representatives regarding the information contained in Moore data shall survive termination of the Agreement. The Company shall indemnify and hold harmless the School Board from and against any loss, claim, cost (including attorneys' fees) or damage of any nature arising from or in connection with the breach by the Company or any of Authorized Representatives of the obligations under this provision.

**Certain Representations and Warranties.** The Company hereby represents and warrants as follows: (a) the Company has full power and authority to execute the Agreement and this MOA and to perform its obligations hereunder and thereunder; (b) the Agreement and this MOA constitute the valid and binding obligations of the Company, enforceable in accordance with their respective terms, except as such enforceability may be limited by bankruptcy or similar laws affecting the rights of creditors and general principles of equity; and (c) the Company's execution and delivery of the Agreement and this Addendum and compliance with their respective terms will not violate or constitute a default under, or require the consent of any third party to, any agreement or court order to which the Company is a party or by which it may be bound.

**Governing Law; Venue.** Notwithstanding any provision contained in the Agreement to the contrary, (a) the Agreement shall be governed by and construed in accordance with the laws of the State of Oklahoma, without reference to conflict of laws principles; and (b) any dispute hereunder which is not otherwise resolved by the parties hereto shall be decided by a court of competent jurisdiction located in the State of Oklahoma.

**IN WITNESS WHEREOF**, the parties hereto have caused this Addendum to be executed by their duly authorized officers effective as of the date first written above.

  
\_\_\_\_\_  
Jun Kim, Director of Technology  
Moore Public Schools 14 Oct 2022

NCS Pearson, Inc.

  
\_\_\_\_\_  
Randall Trask (Aug 17, 2022 14:27 EDT)

Randall Trask  
SVP - Clinical Assessments

Date: 08/17/2022  
\_\_\_\_\_

**ATTACHMENT 1:  
SAMPLE DATA CHECKLIST**

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data- Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	X
	Observation data	
	Other assessment data- Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, preferred or primary language spoken by student)	X

	Other demographic information-Please specify:	[see complete list below]
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	X
	Low income status	X
	Medical alerts	
	Student disability information	X
	Specialized education services (IEP or 504)	X
	Living situations (homeless/foster care)	

# Center for Technology

## Memorandum of Agreement (MOA)

	Other indicator information-Please specify:	[see complete list below]	Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Contact Information	Address		Student Survey Responses	Student responses to surveys or questionnaires	
	Email	X			
	Phone		Student work	Student generated content; writing, pictures etc.	
Student Identifiers	Local (School district) ID number	X		Other student work data Please specify:	
	State ID number	X (optional)			
	Vendor/App assigned student ID number		Transcript	Student course grades	
	Student app username			Student course data	
	Student app passwords			Student course grades/performance scores	
				Other transcript data - Please specify:	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)		Other	Please list each additional data element used, stored or collected by your application	[see complete list below]

Written Specifics by Company from Data Checklist:

**NNAT3 (Assessment Technology Platform – ATP) Data Elements:**

**Student Data Collected (many data elements are optional):**

Student School ID, Student District ID, FirstName, MiddleName, LastName Email, DOB, Gender, IsHispanicLatino, AmericanIndianOrAlaskaNative , Asian , BlackOrAfricanAmerican , NativeHawaiianOtherPacificIslander, White , GradeCode, Student Group Assignment, Start Date, End Date, EC Status, Meal Status, Service Code, ESEA Title, Migrant Education, Special Education IEP, Section 504, Gifted and Talented, After School, Correctional, Summer School, IDEA, Intervention Level, Mobility, Behavior Disorder, Languages Spoken at Home, First Language, Number of Years in US, Number of Years in ELL, Autism, Blindness, Deafness, Deaf-Blindness, Multiple Disabilities, Orthopedic Impairments, Other Health Impairments, Specific Learning Disabilities, Developmental Delay, Emotional Disturbance, Hearing Impairment, Intellectual Disability, Speech or Language Impairment, Traumatic Brain Disorder, Visual Impairment

**User Data Collected:**

Staff Number, LastName, FirstName, Email, SchoolCode, Start Date End Date, User Group Assignment

**ATTACHMENT 2:  
DISPOSITION OF DATA (Sent at Term of Contract)**

Moore Public Schools directs NCS Pearson, Inc. to dispose of data obtained by NCS Pearson, Inc. pursuant to the terms of the MOA between Moore Public Schools and the Company. The terms of the Disposition are set forth below:

**1. Extent of Disposition**

Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

    NNAT3 Student Data. Meta data for system logs is not dispositioned.

\_\_\_ Disposition is Complete. Disposition extends to all categories of data.

**2. Nature of Disposition**

Disposition shall be by destruction or deletion of data.

\_\_\_ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

**[Insert or attach special instructions.]**

**3. Timing of Disposition**

Data shall be disposed of by the following date:

As soon as commercially practicable (or within 60 Days of termination of contract)

\_\_\_ By **[Insert Date]**

**4. Signatures**

\_\_\_\_\_  
(Authorized Representative of Moore)      Date \_\_\_\_\_

**Verification of Disposition of Data**

\_\_\_\_\_  
Authorized Representative of Company      Date \_\_\_\_\_

*N/A @ this  
Time  
14 Oct 2022*

The Moore Public Schools (MPS) Center for Technology Data Privacy and Technology Integration Survey was adapted from the Consortium for School Networking (CoSN) Privacy Toolkit to ensure potential MPS partners understand their duty and responsibility as well as the expectation of MPS regarding cybersecurity, data privacy, and the Family Educational Rights Privacy Act (FERPA) regarding the storage and management of student data. MPS also follows guidance from the [Department of Education Student Data Privacy](#) and from [Access for Learning Community](#).

MPS strives to “Create Connections” for our students and staff – ensuring safe, efficient, and effective operations and communication is central to this process.

**Completion of this survey does NOT guarantee a contract with the vendor or service provider.**

**Please complete this document and email to MPS contact that sent you the survey.**

**DATA PRIVACY AND TECHNOLOGY INTEGRATION SURVEY**

*--To be completed by potential MPS partner--*

Potential Partner Company Name: **NCS Pearson, Inc.**  
Completed Date: **5/17/2022**  
Name of Person Completing: **Matthew Morris**  
Phone of Person Completing: **210-339-5344**  
Email of Person Completing: **matthew.morris@pearson.com**

I affirm that all information below is accurate and true as to our company’s data privacy and integration practices.

Account Representative Name and Signature:   
Randall Trask (Aug 17, 2022 14:27 EDT)

*--If you ONLY provide links to your website and do NOT complete the information requested will be returned and may result in your exclusion for consideration --*

**Data Collection**

Do you **AND** your associated 3<sup>rd</sup> Parties comply with all federal and state requirements like FERPA, COPPA, etc as defined by [Protecting Student Privacy | U.S. Department of Education](#) for any and all functions, such as analytics or PII?

Yes

Do you **AND** your associated 3<sup>rd</sup> Parties **COMPLY** with the General Data Protection Regulation (GDPR)? GDPR became enforceable on May 25, 2018. **Please provide a direct link to your public GDPR policy.**

Yes - <https://www.pearson.com/en-us/legal-information/privacy-policy.html>  
<https://www.pearsonassessments.com/footer/pearson-clinical-privacy-policy.html>

If you **AND/OR** the 3<sup>rd</sup> party does NOT meet above standards, do you assume risk and all associated costs such as mitigating data breach, credit history checks, etc?

N/A

*--If applicable and any of the above answers are “NO”, this potential provider does NOT comply with federal guidance/policy and is a risk to MPS student/staff data. --*

**Data Security and Portability**

Do you guarantee data portability in a usable format of all data elements collected and stored for MPS? What format will you provide this data back to MPS?

**Yes. Upon request in writing from the Customer Account Owner, Pearson can export the customer data in CSV format.**

Do you (including all associated 3<sup>rd</sup> parties) guarantee all data will be deleted with certification upon completion of a contract within 60 days?

**Customers can delete their data at any time using the ATP application. Customer Account Owners must request in writing for Pearson to delete their data. Data would be deleted from the database and would not be usable or accessible within the application, database, or backups.**

Have you experienced any internal or external data breach or cybersecurity event within the last 24 months? If so, what was the issue and please explain action taken to communicate and resolve. **A non-disclosure can be signed as needed.**

**No**

Will any data be stored outside the United States? Where is it stored?

**No**

How is your data at rest encrypted and protected (e.g. just passwords, passwords and sensitive data, all data)?

**Data at rest are encrypted using AES 256.**

If the application is multi-tenant (several districts on one server/instance) hosting, how is data and access separated from other customers in the event of a data breach or event?

**Customer data are logically segregated within the database by customer account.**

How does the provider protect data in transit (e.g. SSL, hashing)?

**Data in transit are encrypted using HTTPS and TLS v1.2.**

Does the provider perform background checks on personnel with administrative access to servers, customer data?  
**You may be required to complete a "Declaration by Vendor" certifying your company has completed a sex offender verification on any employee with access to our student's records or access to our facilities.**

**Yes**

Does the provider perform regular risk assessments, penetration testing, vulnerability management, and intrusion prevention?

**Yes. Risk assessments, vulnerability management, security testing, and intrusion prevention are performed.**

Are backups performed and tested regularly and stored off-site?

**Yes**



**Will you provide certification of data destruction upon completion of contract? MPS requires all data to be provided back to MPS and associated data destroyed on your servers and/or third parties within 60 days of termination of contract.**

Yes

**Instructional Technology (IF APPLICABLE)**

Have you signed the K-12 School Service Provider Pledge to Safeguard Student Privacy 2020? Are you willing to comply and sign the privacy pledge? [Take The Pledge - Student Privacy Pledge | Pledge to Parents & Students](#)

Pearson Clinical Assessments, a business of NCS Pearson, Inc. ("Pearson") recognizes the importance of protecting the privacy of personally identifiable information, while permitting us to conduct legitimate business by providing goods, services and information of interest. Pearson's privacy statement may be viewed at <https://www.pearsonassessments.com/footer/pearson-clinical-privacy-policy.html>. In addition, Pearson is willing to negotiate and execute a mutually agreeable data privacy agreement with respect to the PII of students in the Moore Public Schools.

Have you been vetted by another state educational entity that is part of the [Access for Learning Community](#) or state educational privacy alliance that is part of the COSN network. If so, please identify the state.

Not applicable.

Do you offer Single Sign On (SSO) or Rostering for teacher and/or student accounts? If so, can you work with our current solution(s) with OneRoster, Clever, Kimono, and GG4L **without** modifications or "work-arounds"? Is there an added cost?"

Yes. For SSO: ClassLink, Clever, Google (if username is the email address), and Microsoft (if username is the email address) are supported.

Rostering data can be imported from:

Clever, ClassLink, EDFi, RICone, PowerSchool, OneRoster (v1.1 or v1.2), OneRoster CSV (v1.1 or v1.2)

Integration for Rostering via the above options is done via a separate Pearson application (RaaS)

Does your platform fully integrate with Canvas, Clever, Infinite Campus? Do you charge for these integrations?

No

(If applicable) Does your application allow for grade pass back to Infinite Campus and/or Canvas?

No

Does this program have embedded videos through Youtube, Vimeo, or other streaming sources?

- Are the videos under a specific channel for ease of whitelisting settings?
  - Provide example URL
- Vimeo
- Youtube
- Other: Please identify.

No

Does your instructional platform have stand-alone iOS and Android apps as opposed to accessing via web platform?


No

To be completed by MPS Staff:

- Y /  N – Did the company provide the data checklist (Spreadsheet)
- Y /  N – Does the company adhere to federal/state/district data privacy regulations/guidance?
- Y /  N – Does the company integrate with MPS's current systems?
- Y /  N – Does the company meet the minimum requirements for their data security and implementation?

Reviewed by: \_\_\_\_\_

Date: \_\_\_\_\_

 14 Oct 2022