MAINE STUDENT DATA PRIVACY AGREEMENT
Version 1.0

Maine School Administrative District #6

and

NCS Pearson, Inc.

September 16, 2020

This Maine Student Data Privacy Agreement ("DPA") is entered into by and between the **Maine School Administrative District #6** (hereinafter referred to as "School Unit") and **NCS Pearson, Inc.** (hereinafter referred to as "Provider") on the date provided on the preceding page. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the School Unit with certain digital educational services ("Services") pursuant to a contract dated September 16, 2020 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the School Unit may provide, documents or data that are covered by several federal statutes, among them, the Federal Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. §1232g et. seq. (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. §1232h et. seq.; and Individuals with Disabilities Education Act ("IDEA") 20 U.S.C. § 1400 et. seq. (34 CFR Part 300); and

WHEREAS, the documents and data transferred from School Units and created by the Provider's Services are also subject to several state student privacy laws, including Maine's dissemination of student records law 20-A M.R.S. §6001; Maine Student Information Privacy Act 20-A M.R.S. §951 et. seq. ("MSIPA"); and Maine Unified Special Education Regulations ("MUSER") Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, this Agreement complies with Maine laws, and federal law; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms", agree to allow other school units in Maine the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from the School Unit pursuant to the Service Agreement, including compliance with all applicable federal and state privacy statutes, including FERPA, PPRA, COPPA, IDEA, MSIPA, and MUSER and other applicable Maine laws, all as may be amended from time to time. In performing these Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the School Unit. Provider shall be under the direct control and supervision of the School Unit with respect to the use and maintenance of information shared with Provider by School Unit pursuant to this Agreement and the Service Agreement.

2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational services described below and as may be further outlined in Exhibit "A" hereto:

Please see Exhibit "A" for a description of services for Q-interactive and Q-global platforms on the web-based platform, Digital Assessment Library for Schools (DALS).

3. **Student Data to Be Provided**. In order to perform the Services described in the Service Agreement, School Unit shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Exhibit "B":

- Please see Exhibit "B" for the Schedule of Data including categories of data that may be collected and processed.
- **See Exhibit "B" for additional data that may be provided.**

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over terms used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of School Unit**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the School Unit. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data shall remain the exclusive property of the School Unit. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the School Unit as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access**. School Unit shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. As the School Unit will have access to Student Data through the available functionality of the Services, the School Unit will ordinarily be able to respond to requests to view or correct personally identifiable information in a pupil's records without Provider's assistance; however, the Provider will provide commercially reasonable assistance within ten (10) days after the School Unit's request if the School Unit requires such assistance to view or correct such information.. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the School Unit, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. Provider shall, at the request of the School Unit, provide the School Unit with instructions as to how to use the available functionality of the Services to transfer Student Generated Content to a separate student account. Provider is not responsible for the maintenance of separate accounts for the storage of Student Generated Content or for managing the transfer of such content to any separate accounts maintained by the School Unit or by students.

1. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the School Unit. Provider shall notify the School Unit in advance of a compelled disclosure to a Third Party. The Provider will not use, disclose, compile, transfer, and/or sell the Student Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof without the express written consent of the School Unit or without a court order or lawfully issued subpoena.

1. **No Unauthorized Use**. Provider shall not use Student Data for any purpose other than as explicitly specified in the Service Agreement. Any use of Student Data shall comply with the terms of this DPA.

2. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF SCHOOL UNIT

1. **Provide Data In Compliance With FERPA**. School Unit shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, IDEA, MSIPA, and MUSER and all other Maine privacy statutes and regulations referenced or identified in this DPA.

2. **Annual Notification of Rights.** If the School Unit has a policy of disclosing education records under 34 CFR § 99.31 (a) (1), School Unit shall include a specification of criteria for determining who constitutes a "school official" and what constitutes a "legitimate educational interest" in its annual notification of rights, and determine whether Provider qualifies as a "school official."

3. **Reasonable Precautions**. School Unit shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and hosted data.

4. **Unauthorized Access Notification**. School Unit shall notify Provider promptly of any known or suspected unauthorized access. School Unit will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, IDEA,

MSIPA, MUSER and all other Maine privacy statutes and regulations identified in this DPA.

2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the School Unit unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure**. De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to School Unit, who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data**. To the extent that the School Unit cannot use the product's functionality to delete Student Data themselves, School Unit may request in writing that Provider dispose of or delete Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or to transfer said data to School Unit or School Unit's designee, ninety (90) days after contract expiration. Upon receipt of such notice, nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include: (1) shredding any and all hard copies of any Student Data; and (2) erasing or otherwise modifying the records to make them unreadable and indecipherable. Provider shall provide written notification to School Unit when the Student Data has been disposed of or deleted. The duty to dispose of or delete Student Data shall not extend to data that has been de-identified or placed in a separate student account, pursuant to the other terms of the DPA. The School Unit may employ a "Directive for Disposition of Data" Form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the School Unit, the Provider will immediately provide the School Unit with any specified portion of the Student Data as soon as reasonably practicable after receipt of said request. In the event that provision of data to the School Unit after termination may be impractical, Provider may charge School Unit at Provider's then-current rates for time spent assisting School Unit in extracting or exporting data if such assistance is not included in Provider's standard charges already paid by School Unit for the applicable products or services.

6. **Advertising Prohibition**. Without limiting any other provision in this DPA, Provider is

specifically prohibited from using, disclosing, or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service(s) to School Unit; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service(s) to School Unit.

ARTICLE V: DATA PROVISIONS

1. **<u>Data Security</u>**. The Provider agrees to abide by and maintain commercially reasonable data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in <u>Exhibit "F"</u> hereto. These measures shall include, but are not limited to:

   a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees and contractors with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.

   b. **Destruction of Data**. Upon receipt of written notice from the School Unit or School Unit's designee, Upon receipt of the School Unit's written request, Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and/or transfer said data to School Unit or School Unit's designee, according to a schedule and procedure as the parties may reasonably agree upon. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.

   c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by School Unit.

   d. **Employee Training**. The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide School Unit with contact information of an employee who School Unit may contact if there are any security concerns or questions.

   e. **Security Technology**. When the service is accessed using a supported web browser, Secure Socket Layer ("SSL") or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service

Agreement in an environment using a firewall that is periodically updated according to industry standards.

- **f. Security Coordinator**. Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

- **g. Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

- **h. Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request from School Unit, Provider shall provide School Unit with records evidencing completion of such periodic risk assessments and documenting any identified security and privacy vulnerabilities as well as the remedial measures taken to correct them.

- **i. Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.

- **j. Audits.** Not more than once a year, except in the case of a verified breach, the Provider will allow the School Unit to audit the security and privacy measures that are in place to ensure protection of the Student Data or any portion thereof, subject to reasonable time and manner restrictions. Such audit will be in the form of a written questionnaire that will be supplied by the School Unit to the Provider and to which the Provider will have a reasonable amount of time to respond. Notwithstanding the foregoing, if the Provider has completed an independent third-party audit of its security practices and procedures within the preceding twelve (12) months, from an auditor the School Unit approves of, which approval shall not be unreasonably withheld, the Provider may supply the School Unit with a copy of a summary of the results of such audit in lieu of responding to any audit questionnaire of the School Unit. The Provider will also cooperate reasonably with any state or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or School Unit, and shall provide reasonable access to the Provider's facilities, staff, agents and School Unit's Student Data and all records pertaining to the Provider, School Unit and delivery of Services to the Provider in connection with any such state or federal agency's audit or investigation.

2. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to School Unit within a reasonable amount of time of the incident. Provider shall follow the following process for such notification:

    - **a.** The security breach notification shall be written in plain language, meet all applicable legal requirements and include relevant available information addressing the following areas:

"What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

   i. The name and contact information of the reporting School Unit subject to this section.
   ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
   iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
   iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
   v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. At School Unit's discretion, the security breach notification may also include any of the following:

   i. Information about what the agency has done to protect individuals whose information has been breached.
   ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements in applicable state and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to make a copy of the agreement available to the School Unit in a form that does not compromise the safety or security of Provider's computer systems, and to make staff available at reasonable times to answer questions of School Unit on the written incident response plan.

f. At the request and with the assistance of School Unit, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI- GENERAL OFFER OF TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this to any other School Unit who signs the acceptance on in said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall dispose of and destroy all of School Unit's data pursuant to Article IV, section 5, and Article V, section 1(b).

4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, terms of use, or privacy policy, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives before:

   The designated representative for the Provider for this Agreement is:

Rochelle Snell, K-12 Clinical Assessment Consultant
19500 Bulverde Road, Suite 201, San Antonio, TX 78259
rochelle.snell@pearson.com
612-429-0191

   The designated representative for the School Unit for this Agreement is:

Scott Nason, Director of Technology
290B Parker Farm Road, Buxton, ME 04093
snason@bonnyeagle.org
207-929-2325

6. **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF MAINE, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS IN CUMBERLAND COUNTY, MAINE FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **Authority.** Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way.

10. **Waiver**. No delay or omission of the School Unit to exercise any right hereunder shall be construed as a waiver of any such right and the School Unit reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

[*Signature Page Follows*]

IN WITNESS WHEREOF, the parties have executed this Maine Student Data Privacy Agreement as of the last day noted below.

NCS Pearson, Inc.

BY: Randall T. Trask
Randall T. Trask (Apr 5, 2021 09:09 CDT) Date: 04/05/2021

Printed Name: Randall Trask

Title/Position: Senior Vice President

Address for Notice Purposes:

5601 Green Valley Drive
Bloomington, MN 55437

Maine School Administrative District #6

BY: Scott N Date: 4/6/2021

Printed Name: Scott Nason Title/Position: Director of Technology

Address for Notice Purposes:

290B Parker Farm Road
Buxton, ME 04093

EXHIBIT "A"

DESCRIPTION OF SERVICES

Digital Assessment Library / Q-interactive and Q-global:

The Digital Assessment Library for Schools (DALS) provides a solution for school districts that offers unlimited access to a library of nearly 40 assessments available on Pearson's web-based digital systems, Q-interactive and Q-global.

OOOOO★OOOOO

EXHIBIT "B"

SCHEDULE OF DATA

DATA CATEGORIES

Depending on the Services, we may collect and process the following categories of data in order to manage day to day business needs including, but not limited to, performing services on behalf of a business, payment processing and financial account management, business planning and forecasting, system improvements, security and fraud prevention, and compliance with legal and regulatory obligations:

(A) Identifiers such as a real name, address, unique personal identifiers, or email address
(B) Customer records such as signature
(C) Characteristics of protected classifications under California or federal law
(D) Commercial information, such as products or services purchased, obtained, or considered
(E) Internet or other electronic network activity information such as information regarding a consumer's interaction with an Internet Web site, application, or advertisement
(F) Geolocation data
(G) Sensory data, such as audio, electronic, visual, or similar information
(H) Professional or employment-related information
(I) Education information
(J) Inferences about preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

COLLECTION AND STORAGE OF INFORMATION

We will collect certain personal information during different activities on this Site or otherwise, such as user registration, when you purchase materials, participate in a survey, contact us with questions or offer feedback on the Site. In connection with such activities, you may be asked to provide certain information such as your name, mailing address, telephone number, fax number, credit card number and email address. In order to qualify for the purchase of materials we may also request professional qualifications, affiliations or employment information. We may maintain this information in our computer and ordering system.

PLATFORM AND SYSTEMS INFORMATION

PRODUCT PLATFORM	CATEGORIES OF DATA
Clinical Assessments (Q-global and Q-interactive)	In providing tests and testing services through this system, We collect or receive Personal Information from Examinees, as well as Test Administrators. Certain Examinee Personal Information is provided to us by the Test Administrator; and other information is provided to us by the Examinee. Test Administrator Personal Information is provided to us by the Qualified Customer and the Test Administrator. •Test Administrator Personal Information Collected. The Personal Information that We collect, receive or process with respect to a Test Administrator through this system may include: name, phone number, mobile phone number, email address, Pearson qualification level, log-in ID and password. •Examinee Personal Information Collected. The Personal Information that We collect, receive or process with respect to Examinees may include: first name, last name, Examinee ID (as assigned by a Test Administrator), date of birth, gender, race/ethnicity, handedness and home language. In addition, depending upon the particular clinical assessment, a wide range of additional demographic information may be collected, including, but not limited to: clinical history; education history and issues; work and employment status, history and issues; health conditions; medications; employment status; marital status; family information and history; and living arrangements. Through this system, We collect and score the responses to the clinical assessment questions and derive raw scores and test scaled or percentile scores.

EXHIBIT "C"

DEFINITIONS

METDA (Maine Educational Technology Directors Association): Refers to the membership organization serving educational IT professionals in the state of Maine to promote general recognition of the role of IT professionals in educational institutions; improve network and computer services; integrate emerging technologies; encourage appropriate use of information technology for the improvement of education and support standards whereby common interchanges of electronic information can be accomplished efficiently and effectively.

Covered Information: Covered Information means materials that regard a student that are in any media or format and includes materials as identified by MSIPA. The categories of Covered Information under Maine law are found in Exhibit B. For purposes of this DPA, Covered Information is referred to as Student Data.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or school unit, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs and 504 plans. The categories of Educational Records under Maine law are also found in Exhibit B. For purposes of this DPA, Educational Records are referred to as Student Data.

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Operator: The term "Operator" means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. This term shall encompass the term "Third Party," as it is found in applicable state statues.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by School Unit or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate or combination, would allow a reasonable person who does not have knowledge of the relevant circumstances to be able to identify a student. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the DPA, the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by School Unit and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other School Unit employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records and Covered Information.

Service Agreement: Refers to the Contract or Purchase Order that this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by School Unit or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Massachusetts and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Subscribing School Unit: A School Unit that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than School Unit or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Maine School Administrative District #6 ("School Unit" directs NCS Pearson, Inc. ("Company") to dispose of data obtained by Company pursuant to the terms of the Service Agreement between School Unit and 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:

_____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:

3. Timing of Disposition

Data shall be disposed of by the following date:

_____As soon as commercially practicable

_____By **[Insert Date]**

4. Signature

______________________________ ____________________

Authorized Representative of School Unit Date

5. Verification of Disposition of Data

______________________________ ____________________

Authorized Representative of Company Date

<u>**EXHIBIT "E"**</u>

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and **Maine School Administrative District #6** and which is date September 16, 2020 to any other School Unit ("Subscribing School Unit") who accepts this General Offer though its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other School Unit may also agree to change the data provide by School Unit to the Provider to suit the unique needs of the School Unit. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the either the METDA or SDPC in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

Provider Name: **NCS Pearson, Inc.**

BY: Randall T. Trask
Randall T. Trask (Apr 5, 2021 09:09 CDT)

Date: 04/05/2021

Printed Name: Randall T. Trask

Title/Position: Sr. Vice President

2. Subscribing School Unit

A Subscribing School Unit, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing School Unit and the Provider shall therefore be bound by the same terms of this DPA.

BY: ____________________

Date: ____________________

Printed Name: ____________________

Title/Position ____________________

EXHIBIT "F" DATA SECURITY REQUIREMENTS

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]