

**NEW HAMPSHIRE STUDENT DATA PRIVACY AGREEMENT  
VERSION (2019)**

**Concord School District**

**and**

**NCS Pearson, Inc.**

**December 2, 2020**

This New Hampshire Student Data Privacy Agreement (“DPA”) is entered into by and between the school district, Concord School District (hereinafter referred to as “LEA”) and NCS Pearson, Inc. (hereinafter referred to as “Provider”) on December 2, 2020. The Parties agree to the terms as stated herein.

## **RECITALS**

**WHEREAS**, the Provider has agreed or will agree to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) as described in Article I and Exhibit “A”; and

**WHEREAS**, the Provider, by signing this Agreement, agrees to allow the LEA to offer school districts in New Hampshire the opportunity to accept and enjoy the benefits of the DPA for the Services described, without the need to negotiate terms in a separate DPA; and

**WHEREAS**, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g and 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; the Individuals with Disabilities Education Act (“IDEA”), 20 U.S.C. §§ 1400 et. seq., 34 C.F.R. Part 300; and

**WHEREAS**, the documents and data transferred from New Hampshire LEAs and created by the Provider’s Services are also subject to several New Hampshire student privacy laws, including RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

**WHEREAS**, the Parties wish to enter into this DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

**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 (as defined in Exhibit “C”) transmitted to Provider from the LEA pursuant to Exhibit “A”, including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, SOPIPA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100; and other applicable New Hampshire state laws, all as may be amended from time to time. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit “C”) from Pupil Records (as defined in Exhibit “C”) are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.
  
2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational services described in Exhibit “A”.

3. **Student Data to Be Provided.** In order to perform the Services described in this Article and Exhibit “A”, LEA shall provide the categories of data described in the Schedule of Data, attached hereto as Exhibit “B”. The Provider may update the categories of data collected in Exhibit B after execution of this Agreement by providing notice to the LEA (and Subscribing LEAs applicable) of the updated categories of Student Data collected through a revised Exhibit B, which will thereafter become a part of the DPA and supersede the prior Exhibit B.
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 all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

## **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Student Data Property of LEA.** All Student Data or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA , or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of student data notwithstanding the above. The LEA will generally have access to any Student Data it desires through the available functionality of the Services. In the event that the LEA requires assistance for access or extraction, Provider will provide commercially reasonable assistance within ten (10) days of the LEA’s request.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information 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 LEA will have access to Student Data through the available functionality of the Services, the LEA 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 LEA’s request if the LEA 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 Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** Provider shall, at the request of the LEA, provide the LEA with instructions as to how to use the available functionality of the Services to export or download Student

Generated Content that is severable from the Services. 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 LEA or by students.

4. **Third Party Request.** Should a Third Party, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, 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 LEA and shall cooperate with the LEA to collect the required information. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. The Provider will not use, disclose, compile, transfer, 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 LEA or without a court order or lawfully issued subpoena. The prohibition in the prior sentence does not apply to Subprocessors assisting the Provider in providing services under this DPA or assisting the Provider in developing, researching, and improving educational sites, services, or applications. 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.
5. **No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in this DPA.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

### **ARTICLE III: DUTIES OF LEA**

1. **Provide Data In Compliance With Laws.** LEA shall provide data for the purposes of the DPA in compliance with the FERPA, PPRA, IDEA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and the other privacy statutes quoted in this DPA. LEA shall ensure that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials."
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
3. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA 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 New Hampshire and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and all other applicable New Hampshire privacy statutes and regulations.
- 2. Authorized Use.** Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than the Services stated in this DPA and as 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, any student data, 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 LEA, 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 this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DPA.
- 4. No Disclosure.** De-identified information, as defined in Exhibit “C”, 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 the LEA who has provided prior written consent for such transfer. The prohibition in the prior sentence does not apply to Subprocessors assisting the Provider in providing services under this DPA or assisting the Provider in developing, researching, and improving educational sites, services, or applications. Provider shall not copy, reproduce or transmit any Student Data obtained under this DPA and/or any portion thereof, except as necessary to fulfill the DPA. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA’s written approval of the manner in which de-identified data is presented
- 5. Disposition of Data.** Provider shall dispose or delete all Student Data obtained under the Agreement within thirty (30) days after the LEA makes a written request for deletion. The LEA is responsible for extracting any data it wishes to keep through the standard functionality of the Services. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means or de-identified consistent with the provisions of 34 CFR 99.31(b). Nothing in this DPA authorizes Provider to maintain Student Data obtained under the DPA beyond the time period reasonably needed to complete the

disposition. Upon the LEA's written request, Provider shall provide written confirmation to LEA when the Student Data has been disposed. The duty to dispose of 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 LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LEA, the Provider will provide reasonable assistance to the LEA in using the available functionality of the Services to export Student Data stored within the Services."

6. **Advertising Prohibition.** Provider is prohibited from leasing, renting, using 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 to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to Client. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes or modify the provisions of Article IV, Section 4 of this Agreement.

## **ARTICLE V: DATA PROVISIONS**

1. **Data Security.** The Provider agrees to abide by and maintain adequate 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 Exhibit "F" 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 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.** Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the DPA when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the DPA authorizes Provider to maintain personally identifiable 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 DPA in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the DPA, except as necessary to fulfill the purpose of data requests by LEA. The foregoing does not limit the ability of the Provider to allow any necessary service providers to view or access data as set forth in Article IV, section 4.

- d. **Employee Training.** The Provider shall provide recurring, periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA 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 DPA in an environment using a firewall that is periodically updated according to industry standards.
- f. **Security Coordinator.** Upon request, Provider shall provide the name and contact information of Provider’s Security Coordinator for the Student Data received pursuant to the DPA.
- 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.
- 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 LEA 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 LEA 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 LEA approves of, which approval shall not be unreasonably withheld, the Provider may supply the LEA with a copy of a summary of the results of such audit in lieu of responding to any audit questionnaire of the LEA. 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 LEA, and shall provide reasonable access to the Provider’s facilities, staff, agents and LEA’s Student Data and all records pertaining to the Provider, LEA and delivery of Services to the Provider in connection with any such state or federal agency’s audit or investigation.
- k. **New Hampshire Specific Data Security Requirements.** The Provider agrees to the following privacy and security standards from “the Minimum Standards for Privacy and Security of Student and Employee Data” from the New Hampshire Department of Education. Specifically, the Provider agrees to:
  - (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
  - (2) Limit unsuccessful logon attempts;

- (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
- (4) Authorize wireless access prior to allowing such connections;
- (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
- (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
- (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
- (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
- (9) Enforce a minimum password complexity and change of characters when new passwords are created;
- (10) Perform maintenance on organizational systems;
- (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
- (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data in accordance with NIST SP 800-88 Revision 1;
- (13) Protect (i.e., physically control and securely store) system media containing Student Data, both paper and digital;
- (14) Sanitize or destroy system media containing Student Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
- (15) Control access to media containing Student Data and maintain accountability for media during transport outside of controlled areas;
- (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;
- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;



- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

**2. Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA as soon as practicable and no later than ten (10) days of confirmation that an incident has occurred. Provider shall follow the following process:

- a.** The security breach notification shall be written in plain language, meet all applicable legal requirements and include relevant available information addressing the questions of: “What Happened,” “What Information Was Involved,” “When it Occurred,” “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 LEA 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.
  - vi.** If the information is possible to determine at the time notice is provided, the estimated number of students and teachers affected by the breach, if any.
- c.** At LEA’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 the New Hampshire Data Breach law 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 staff available at reasonable times to answer questions of LEA on the written incident response plan.
  - a. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access arising from the failure of Provider to comply with the requirements of this DPA and such assistance is not unduly burdensome to Provider, Provider shall assist LEA in notifying the affected parent, legal guardian or eligible pupil of the unauthorized access and reimburse LEA for reasonable costs incurred to provide legally required notifications.
- b.

## ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for three (3) years.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated.

The LEA may terminate this DPA and any service agreement or contract with the Provider if the Provider breaches any terms of this DPA.

3. **Effect of Termination Survival**. If the DPA is terminated, the Provider shall destroy all of LEA's data pursuant to 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, IDEA, COPPA, PPRA, RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100. In the event there is conflict between the terms of the DPA and any other writing, such as service agreement or with any other bid/RFP, terms of service, privacy policy, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other 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 below.

The designated representative for the Provider for this Agreement is:

Name      NCS Pearson, Inc.  
Title      Clinical Assessment  
Address    19500 Bulverde Road, Suite 201, San Antonio, TX 78259  
Telephone (800) 627-7271  
Email      catalogbidsandproposals@pearson.com

The designated representative for the LEA for this Agreement is:

Pam McLeod, CETL  
Director of Technology | Concord School District  
38 Liberty Street, Concord, NH 03301  
(603) 225.0811  
pmcleod@sau8.org

- 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 NEW HAMPSHIRE, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF MERRIMACK COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA 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 LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.
11. **Multiple Counterparts:** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart.


## ARTICLE VII- 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 district who signs the acceptance in said Exhibit.

*[Signature Page Follows]*

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

**CONCORD SCHOOL DISTRICT**

By:  Date: 12/06/2020  
Pamela McLeod (Dec 5, 2020 17:52 EST)

Printed Name: Pamela R McLeod Title/Position: Director of Technology

**NCS PEARSON, INC.**

By: *Randall T. Trask* Date: 12/02/2020  
Randall T. Trask (Dec 2, 2020 19:34 CST)

Printed Name: Randall T. Trask Title/Position: Senior VP

**EXHIBIT “A”**  
**DESCRIPTION OF SERVICES**

<b>PLATFORM</b>	<b>COVERED PRODUCTS</b>
Assessment Technology Platform	NNAT3, Grade, Gmade, TELL
TEP/Program Workshop	SAT, OLSAT, NNAT2
AimswebPlus	AimswebPlus
Review360	Review360
Work Sampling Online / Ounce	Work Sampling Online / Ounce
DRA2	DRA2
DRA3	DRA3
WriteToLearn	WriteToLearn
Q-Global	{NEED A WAY TO DEFINE}
Q-Interactive	{NEED A WAY TO DEFINE}

**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**

Platform specific data collection is described in the table below:

<b>PRODUCT PLATFORM</b>	<b>CATEGORIES OF DATA</b>
-------------------------	---------------------------

<p>Clinical Assessments (Q-Global and Q-interactive)</p>	<p>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.</p> <ul style="list-style-type: none"> <li>•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.</li> <li>•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.</li> </ul>
<p>AimswebPlus</p>	<p>Educator: To create a record for a student the following information must be collected from educators through this Site: student’s name, grade, birth date, gender, student identification number, district, school, service code, ethnicity and free and reduced lunch status. The following additional information may be collected: Entry Grade, IEP, ESL, Section 504, After School, Correctional, Summer School, IDEA, Gifted/Talented, Intervention Level, Mobility, Behavior Disorder, Federal Disability Categories. Upon initial login by an educator the following personal information may be collected: name, school district, address, phone number, and email. If Pearson receives inquiries or emails about or through this Site from educators, Pearson may keep a record of the email, correspondence and comments, including the individual’s name, school district or organization name and email address in order to reply to the communication, perform Site support and issue resolution and maintain business records concerning this Site. <b>THE ENTRY OF ALL STUDENT PERSONAL DATA IS THE SCHOOL'S RESPONSIBILITY AND PEARSON ASSUMES NO RESPONSIBILITY TO ENTER, COLLECT, OR REVIEW ANY SUCH DATA.</b></p>



	<ul style="list-style-type: none"> <li>• <b>Student Data:</b> Students cannot access aimswebPlus. Any required student testing is conducted in a separate test platform, TestNav. Once a student completes testing in TestNav the student testing data is transferred to aimswebPlus. Student testing data can be reported to Parents as a pdf file extract from aimswebPlus.</li> <li>• <b>Parents and Students:</b> Pearson cannot collect personal information directly from parents or students through this website. Parents and students will not have login or access to AimswebPlus. Parents and students may receive PDF report extracts from an educator.</li> </ul>
<p>Development Reading Assessment (DRA)</p>	<ul style="list-style-type: none"> <li>• <b>Administrators:</b> Each school using the Site must designate an administrator, whose name is provided to the Site. The administrator also provides us with the following data for the administrator: office phone, birthdate and email address. We are also provided with the name of the school district, the name of the school, and the city, county, and zip code of that school. We collect from the administrator the full names of educators that the administrator has decided should be eligible to use the Site. Once entered, each such educator is assigned a user identification and password, enabling them to log onto the Site and to enter or modify student DRA assessment data for students in their class. An administrator may automatically import student data into the Site if the school or district has such files stored or otherwise available electronically. <b>THE ENTRY OF ALL STUDENT PERSONAL DATA OR DRA ASSESSMENT DATA IS THE SCHOOL’S RESPONSIBILITY AND PEARSON ASSUMES NO RESPONSIBILITY TO ENTER, COLLECT, OR REVIEW ANY SUCH DATA.</b></li> <li>• <b>Educators:</b> Educators with User IDs and passwords may log onto the Site. If the administrator has not imported or otherwise entered the following information regarding the educator's classes and students, educators are asked to manually enter their students’ full names, birthdates, grade, gender, student ID, and any special education and bilingual classifications.</li> <li>• <b>View-Only Access Users:</b> Other school or district officials that require view-only access shall be given access to DRA assessment data upon registration. View-only access users may only view DRA assessment data and may not modify or otherwise change any data on the Site. We will collect the name, email address, birthdate and work phone number when registering any view-only access user.</li> <li>• <b>Students:</b> Except for collecting the student information from a school official or educator for purposes of correlating DRA assessment data to such student, the Site does not request or collect any other personal information regarding students from the schools, administrators, educators, students or parents. In no event do we ask children or students for any personal information directly either online or offline.</li> </ul>

	<ul style="list-style-type: none"> <li>•</li> </ul>
Review360	<p>We collect a limited amount of personal information from educators, administrators, parents and non-registered users ("Users") about themselves and their students in order to be able to provide the services through the Site in connection with Review 360. This Site is only intended for use by educators in schools and/or school districts or related entities (collectively, "Schools"), and is not intended for use by the student. In no event do we ask students for any personal information directly either online or offline.</p> <ul style="list-style-type: none"> <li>• Administrators: Each Review 360 licensee using the Site must designate at least one License Manager, whose name is provided to the Site. The License Manager also provides us with the necessary contact information for the administrator. The License Manager will be responsible for setting up all applicable professionals utilizing this License. License Managers are also responsible for creating additional administrator and professional-level accounts. Once entered, each such User is assigned a user identification and password, enabling them to log onto the Site and to enter or modify student Review 360 data for students. THE ENTRY OF ALL STUDENT PERSONAL DATA IS THE SCHOOL'S RESPONSIBILITY AND PEARSON ASSUMES NO RESPONSIBILITY TO ENTER, COLLECT, OR REVIEW ANY SUCH DATA.</li> <li>• Educators: Educators with User IDs and passwords may log onto the Site. If a license/program/site administrator has not imported or otherwise entered the following information regarding the educator's classes and students, educators are asked to manually enter their students' information. To create a record for a student, you need to supply us with the student's grade, unique student number, and campus of registration (this information is used to personalize the content of the Site). In addition, if you are registering as an educator or a school, you also have the option of supplying us with the following information: the student's first language, ethnicity and class level, as well as telling us whether the student participates in an Individualized Education Program (IEP), or any other customized demographics that your school or district asks to collect.</li> <li>• Students: Except for collecting the student information from a school official or educator as required for recording information, the Site does not request or collect any other personal information regarding students from the schools, administrators, educators, students or parents. In no event do we ask students for any personal information directly either online or offline.</li> </ul>
WriteToLearn	<p>Student responses from WriteToLearn activities are collected and scored automatically. Through this Site, the School, through the student's educator</p>

	(as designated on the Student Enrollment file), may obtain and print reports about the results for that student and track such student's learning progress.
Ounce and Work Sampling	<p>We collect a limited amount of personal information from educators, administrators, parents and non-registered users about themselves and their students in order to be able to provide the services through the Site in connection with Work Sampling Online and Ounce Online. This Site is only intended for use by parents or guardians and educators, schools and/or school districts (collectively, "Schools"), and is not intended for use by the student. In no event do we ask children or students for any personal information directly either online or offline.</p> <ul style="list-style-type: none"> <li>• Administrators: Each Work Sampling Online and Ounce Online licensee using the Site must designate at least one License Manager, whose name is provided to the Site. The License Manager also provides us with the necessary contact information for the administrator. The License Manager will be responsible for setting up all applicable districts and schools utilizing this License. License Managers are also responsible for creating additional administrator and educator accounts. Once entered, each such User is assigned a user identification and password, enabling them to log onto the Site and to enter or modify student Work Sampling Online and Ounce Online assessment data for students in their class(es). <b>THE ENTRY OF ALL STUDENT PERSONAL DATA OR WORK SAMPLING ONLINE OR OUNCE ONLINE ASSESSMENT DATA IS THE SCHOOL'S RESPONSIBILITY AND PEARSON ASSUMES NO RESPONSIBILITY TO ENTER, COLLECT, OR REVIEW ANY SUCH DATA.</b></li> <li>• Educators: Educators with Users IDs and passwords may log onto the Site. If an administrator has not imported or otherwise entered the following information regarding the educator's classes and students, educators are asked to manually enter their students' information. To create a record for a student, you need to supply us with the student's name, birth date, and gender (this information is used to personalize the content of the Site). In addition, if you are registering as an educator or a school, you also have the option of supplying us with the following information: the student's first language, ethnicity and class level, as well as telling us whether the student participates in an Individualized Education Program (IEP), or any other customized demographics that your school or district asks to collect. Such optional information would be used solely to create aggregated non-personalized outcome group progress reports that may be desired by an administrator or a school district.</li> <li>• Guest: As a guest, you may take a tour of the Site, as well as read information on the different applications available on the Site. This requires neither</li> </ul>

	<p>registration nor log in, and we do not ask for any personal information from guests.</p> <ul style="list-style-type: none"> <li>• Students: Except for collecting the student information from a school official or educator for purposes of correlating Work Sampling Online and Ounce Online assessment data to such student, the Site does not request or collect any other personal information regarding students from the schools, administrators, educators, students or parents. In no event do we ask children or students for any personal information directly either online or offline.</li> <li>• Testing Information: Developmental Checklists and other individual reports are inputted (or otherwise imported) by the educator into the Site and are accessible only to educators, administrators or other authorized school official.</li> </ul>
<p>Assessment Technology Platform (ATP): TELL, NNAT, GMADE / GRADE</p>	<ul style="list-style-type: none"> <li>• Administrators: To create an Assessment Program record for a student and register students for an assessment in that Assessment Program, the following information may be collected from educators through this Site, as specified by the Education Agency sponsoring the Assessment Program: student's name, birth date, gender, statewide identifier, student's first language, ethnicity, grade level, participation in an Individualized Education Program (IEP). Other demographic information may also be collected if so specified by the Education Agency for the Assessment Program. To order materials related to an Assessment Program, the following personal information may be collected: name, school district, address, phone number, and quantity. If Pearson receives inquiries or emails about or through this Site from educators, Pearson may keep a record of the email, correspondence and comments, including the individual's name, school district or organization name and email address in order to reply to the communication, perform Site support and issue resolution and maintain business records concerning this Site.</li> <li>• Parents and Students: At this time, Pearson does not seek to collect personal information from parents or students through this website.</li> </ul>

**EXHIBIT “C”**

**DEFINITIONS**

**De-Identifiable Information (DII):** De-Identification refers to the process by which the Vendor 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. The Provider’s specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual.

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

**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 LEA or its users, students, or students’ parents/guardians. PII includes, without limitation, at least the following:

- |   |                             |
|---|-----------------------------|
| First Name  | Home Address                |
| Last Name   | Subject                     |
| Telephone Number  | Email Address               |
| Discipline Records  | Test Results                |
| Special Education Data  | Juvenile Dependency Records |
| Grades  | Evaluations                 |
| Criminal Records  | Medical Records             |
| Health Records  | Social Security Number      |
| Biometric Information   | Disabilities                |
| Socioeconomic Information   | Food Purchases              |
| Political Affiliations  | Religious Information       |
| Text Messages   | Documents                   |
| Student Identifiers   | Search Activity             |
| Photos  | Voice Recordings            |
| Videos  | Date of Birth               |
| Grade   | Classes                     |
| Place of birth  | Social Media Address        |
| Unique pupil identifier   |                             |
| Credit card account number, insurance account number, and financial services account number |                             |
| Name of the student's parents or other family members                                       |                             |

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email

**Provider:** For purposes of the DPA, 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.

**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 LEA 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 local educational LEA employee.

**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. The definition of "school official" encompasses the definition of "authorized school personnel" under 603 CMR 23.02.

**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA 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, the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number, student identifiers, 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 New Hampshire and Federal laws and regulations. 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. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services.

**Subscribing LEA:** An LEA 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 LEA 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 an entity that is not the provider or LEA.

**EXHIBIT "D"**

**DIRECTIVE FOR DISPOSITION OF DATA**

[Name or District or LEA] directs [Name of Company] to dispose of data obtained by Company pursuant to the terms of the DPA between LEA and Provider. 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:

[Insert categories of data here]

\_\_\_ 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

\_\_\_ By (Insert Date)

4. Signature

\_\_\_\_\_  
(Authorized Representative of LEA)

\_\_\_\_\_  
Date

5. Verification of Disposition of Data

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

\_\_\_\_\_  
Date



**OPTIONAL: EXHIBIT “F”**

**DATA SECURITY REQUIREMENTS**

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy?  Yes  No

If yes, please provide it.

2. Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

ISO 27001/27002

CIS Critical Security Controls

NIST Framework for Improving Critical Infrastructure Security

Other: \_\_\_\_\_

3. Does your organization store any customer data outside the United States?  Yes  No

4. Does your organization encrypt customer data both in transit and at rest?  Yes  No

5. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

Name: Rod Wallace

Contact information: (210) 305-2521 \_\_\_\_\_

6. Please provide any additional information that you desire.






# Pearson\_ConcordNH

Final Audit Report

2020-12-05

Created:	2020-12-05
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAG-PTW6FQ55IJQKCrxZ2lwObxuQ8l8eVO

## "Pearson\_ConcordNH" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)  
2020-12-05 - 10:01:09 PM GMT- IP address: 159.117.176.208
-  Document emailed to Pamela McLeod (pmcleod@sau8.org) for signature  
2020-12-05 - 10:03:12 PM GMT
-  Email viewed by Pamela McLeod (pmcleod@sau8.org)  
2020-12-05 - 10:51:26 PM GMT- IP address: 104.47.56.254
-  Document e-signed by Pamela McLeod (pmcleod@sau8.org)  
Signature Date: 2020-12-05 - 10:52:16 PM GMT - Time Source: server- IP address: 69.131.4.35
-  Agreement completed.  
2020-12-05 - 10:52:16 PM GMT