

**STANDARD STUDENT DATA PRIVACY AGREEMENT**

**NEW HAMPSHIRE**

**NH-DPA, Modified Version 1.0**

**MANCHESTER SCHOOL DISTRICT – SAU 37**

**and**

**POWERSCHOOL GROUP LLC**

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: Manchester School District – SAU 37, located at 20 Hecker Street, Manchester, New Hampshire 03064 (the “**Local Education Agency**” or “**LEA**”) and PowerSchool Group LLC, located at 150 Parkshore Dr., Folsom, CA 95630 (the “**Provider**”).

**WHEREAS**, the Provider is providing educational or digital services to LEA.

**WHEREAS**, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

**WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

**NOW THEREFORE**, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
  - If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
  - If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

**The designated representative for the Provider for this DPA is:**

General Counsel  
PowerSchool Group LLC  
150 Parkshore Drive, Folsom CA 95630  
legalnotices@powerschool.com

**The designated representative for the LEA for this DPA is:**

Stephen P. Cross, CIO  
[scross@mansd.org](mailto:scross@mansd.org)  
20 Hecker Street  
Manchester, NH 03064  
603-624-6300 x162

**IN WITNESS WHEREOF**, LEA and Provider execute this DPA as of the Effective Date.

**MANCHESTER SCHOOL DISTRICT – SAU 37**

  
STEPHEN CROSS (Jul 5, 2024 23:09 EDT)

By: \_\_\_\_\_

Date: 07/05/24

Printed Name: Stephen Cross

Title/Position: CIO

**POWERSCHOOL GROUP LLC**

By:  \_\_\_\_\_

Date: July 3, 2024

Printed Name: Eric Shander

Title/Position: Chief Financial Officer

## **STANDARD CLAUSES**

Version 1.0

### **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 including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, 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 LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
- 2. Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
- 3. 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 any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

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

- 1. Student Data Property of LEA.** 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 LEA. 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 contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
- 2. PowerSchool created metadata:** Operation of PowerSchool systems creates metadata. Metadata is necessary to monitor the health and security of PowerSchool systems and to provide customer support. Metadata is necessary for answering customer questions about the use of PowerSchool systems by customer users, and for some products, providing the customer with an administrative dashboard. Because the definition of FERPA PII is very broad, some PowerSchool created metadata necessarily contains FERPA PII. The FERPA PII contained in PowerSchool created metadata is a copy of customer data and not a subtraction from customer data. PowerSchool protects metadata that contains FERPA PII as if it were customer data. There are a few notable differences in the treatment of PowerSchool metadata containing FERPA PII than the treatment of customer data. PowerSchool metadata, depending on the storage mechanism, such as a log file, will be overwritten over time. PowerSchool metadata is not saved for returning and is not returned to the customer at the end of the agreement. PowerSchool metadata may be kept for 90 days after termination of the agreement for security purposes. Some PowerSchool products may have data minimization plans that keep product specific metadata longer than 90 days; in such a case, PowerSchool metadata which includes FERPA PII will be kept no longer than fourteen (14) months. PowerSchool proprietary metadata remains the property of PowerSchool.
- 3. Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a

parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student 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 LEA, who will follow the necessary and proper procedures regarding the requested information.

**4. Intentionally Omitted.**

**5. Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

**6. Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the material terms of this DPA.

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

**1. Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

**2. Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA 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.

**3. Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

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

**5. Security Protocols and Training.** LEA agrees to maintain commercially reasonable security protocols that address the collection and transmission of Student Data while using or accessing the Services, including ensuring that Student Data may only be viewed or accessed by parties legally allowed to do so. LEA acknowledges the importance of providing cybersecurity training to its users. Accordingly, LEA will in good faith consider developing cybersecurity training for its staff and other users in the future.

### **ARTICLE IV: DUTIES OF PROVIDER**

**1. Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and

regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services described in the Service Agreement and further outlined in Exhibit A or as otherwise authorized under applicable law.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student 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.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not sell Student Data to any third party.
5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA or any other applicable laws and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services, including Subprocessors or third parties working in collaboration with Provider for this purpose; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors or third parties working in collaboration with Provider for the purposes described in this paragraph or in the DPA, Provider agrees not to transfer de-identified Student Data to any third party. 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.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA

employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

## ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** The Provider will make available to LEA, as soon as possible following the date hereof and at least once every calendar year thereafter, Provider's ISO/IEC 27001 Statement of Applicability (the "SOA"), ISO 27001 certificate issued by the relevant certification body, or equivalent documents relative to an accepted alternative security program and relative to the applicable product or services. Upon LEA's written request, the Provider will: (a) provide access to such documents to any state or federal agency with oversight authority or jurisdiction in connection with any investigation of the Provider and/or the delivery of Services to students and/or LEA; and (b) reasonably cooperate with such state or federal agency in connection with any such investigation.
3. **Data Security.** The Provider agrees to utilize commercially reasonable administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The Provider's Cybersecurity Framework is aligned with the nationally recognized standard selected in **Exhibit "F"**, subject to appropriate exclusions, variations, or exemptions as determined by Provider. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within the most expedient time possible and without unreasonable delay, but no later than five (5) calendar days, unless specified differently in Exhibit G, after the determination that a breach has occurred, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
  - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
    - 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; and
    - v. A general description of the breach incident, if that information is possible to determine

at the time the notice is provided.

- (2) Provider agrees to adhere to all applicable federal and state requirements 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.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects reasonable 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 provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and known facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure Student Data.

#### **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 **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

#### **ARTICLE VII: MISCELLANEOUS**

1. **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. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, or writing, the terms of this DPA shall apply and take precedence. Either party may terminate this DPA and any service agreement or contract if the other party breaches any material terms of this DPA and the breaching party fails to cure such breach within thirty (30) days.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data 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, Terms of Service, Privacy Policies, or with any other bid/RFP, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute 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.

5. **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.
  
6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
  
7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA (the "Successor"), the Provider shall provide written communication to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such communication shall include a written, signed assurance that the Successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. Subject to the terms of this Section 7, the LEA has the right to terminate the DPA and Service Agreement upon providing written notice to the Provider and, if known, to the Successor, if: (a) the LEA reasonably believes, supported by reasonable documentation, that the Successor cannot uphold the material terms and conditions under such agreements; provided that the Provider or the Successor shall have thirty (30) business days from receipt of the termination notice to demonstrate to the LEA the Successor's ability to perform under the Service Agreement and the DPA; or (b) having a DPA with the Successor would violate the LEA's then-current written policies or any applicable state or federal law. The LEA's right to terminate under this Section 7 shall expire ninety (90) days after the closing date of the sale, merger or disposal. If the LEA fails to timely exercise its right to termination during such ninety (90) day period, LEA shall have no further right to terminate pursuant to this Section 7. In the event of termination under this Section 7, the LEA shall be obligated to pay for any and all services provided up to the effective date of termination, and shall not be entitled to a refund or credit of any amounts paid by the LEA to the Provider (or the Successor) for any and all services provided up to the effective date of termination.
  
8. **Authority**. Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein.
  
9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

**EXHIBIT "A"**

**DESCRIPTION OF SERVICES**

The descriptions of the PowerSchool products can be found at:

[Microsoft Word - EXHIBIT A - Product Descriptions \(powerschool.com\)](#)

**EXHIBIT "B"**  
**SCHEDULE OF DATA**

The data elements for the PowerSchool products can be found at:  
[Microsoft Word - EXHIBIT B - Total \(powerschool.com\)](#)

## **EXHIBIT "C"** **DEFINITIONS**

**De-Identified Data and De-Identification:** Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

**Educational Records\*:** Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, 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.

**Metadata:** means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation. Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

**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 for K-12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

**Originating LEA:** An LEA who originally executes the DPA in its entirety with the Provider.

**Provider:** For purposes of the DPA, the term "Provider" means the party identified as 'Provider' in the DPA.

**Student Generated Content\*:** The term "student-generated content" means materials or content created by a student in the services 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 student content.

**School Official:** For the purposes of this DPA 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 Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

**Service Agreement:** Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

**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, birthdate, home or other physical

address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local 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.

**Subprocessor:** For the purposes of this DPA, 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 service, and who has access to Student Data.

**Subscribing LEA:** An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

**Targeted Advertising:** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

**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 Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

\* Notwithstanding the definitions provided for "Educational Records", "Student Generated Content" and "Student Data", they shall be construed consistently with and not to exceed the scope of how such terms (or substantially similar terms) are defined under applicable laws, including FERPA (for "Student Generated Content") with FERPA as the first order of precedence.

**EXHIBIT "D"**  
**DIRECTIVE FOR DISPOSITION OF DATA**

**[Insert Name of District or LEA]** Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement 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. Schedule 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

**EXHIBIT “F”**  
**DATA SECURITY REQUIREMENTS**

**Adequate Cybersecurity Frameworks**  
**2/24/2020**

The Education Security and Privacy Exchange (“Edspex”) works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles\* (“Cybersecurity Frameworks”) that may be utilized by Provider.

Cybersecurity Frameworks

	<b>MAINTAINING ORGANIZATION/GROUP</b>	<b>FRAMEWORK(S)</b>
	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
X	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

\*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

**EXHIBIT "G"**

**New Hampshire**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the 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;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

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

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.  
Date of birth.  
Personal street address.  
Personal email address.  
Personal telephone number  
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required".
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) engage in targeted advertising; (c) develop a profile of a student for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as

necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes. This section does not prohibit Provider from using De-Identified Data in accordance with the terms of this Agreement. For the avoidance of doubt, Student Data and Teacher Data do not include De-Identified Data, and nothing in this DPA precludes Provider from using De-Identified Data.

7. The Provider can demonstrate and will continue to demonstrate successful completion of ISO/IEC 27001:2013 standard and can provide a successful certification upon written request for Provider's Services.
8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information if known by the Provider:
  - i. The estimated number of students and teachers affected by the breach, if any.

The parties agree to add the following categories into the definition of Student Data: 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.

**EXHIBIT "H"**  
**Additional Terms or Modifications**  
*Version 1.0*

LEA and Provider agree to the following additional terms and modifications:

Notwithstanding anything in the contrary in the DPA or other Exhibits thereto, LEA and Provider agree to the following terms and modifications:

None

**EXHIBIT "I"**

**SCHEDULE OF TEACHER DATA**

<b>Category of Data</b>	<b>Elements</b>	<b>Check if used by your system</b>
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	X
Application Use Statistics	Meta data on user interaction with application	X
Communications	Online communications that are captured (emails, blog entries}	X
Demographics	Date of Birth	X
	Place of Birth	X
	Social Security Number	X
	Ethnicity or race	X
	Other demographic information-Please specify:	X
Personal Contact Information	Personal Address	X
	Personal Email	X
	Personal Phone	X
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	X
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district} ID number	X
	State ID number	X
	Vendor/App assigned student ID number	X
	Teacher app username	X
	Teacher app passwords	X
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	X
	Other teacher work data -Please specify:	X
Education	Course grades from schooling	

\*Not all data elements checked above are processed by every Service provided by Provider.

# PowerSchool\_ManchesterDPA\_NH\_Only\_VendorSigned

Final Audit Report

2024-07-06

Created:	2024-07-04
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAR9eiMqvKSZcoB_N2nVNQOiSpgs5yulf

## "PowerSchool\_ManchesterDPA\_NH\_Only\_VendorSigned" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)  
2024-07-04 - 6:29:51 PM GMT
-  Document emailed to STEVE CROSS (scross@mansd.org) for signature  
2024-07-04 - 6:29:56 PM GMT
-  Email viewed by STEVE CROSS (scross@mansd.org)  
2024-07-06 - 3:07:37 AM GMT
-  Signer STEVE CROSS (scross@mansd.org) entered name at signing as STEPHEN CROSS  
2024-07-06 - 3:09:43 AM GMT
-  Document e-signed by STEPHEN CROSS (scross@mansd.org)  
Signature Date: 2024-07-06 - 3:09:45 AM GMT - Time Source: server
-  Agreement completed.  
2024-07-06 - 3:09:45 AM GMT