STANDARD STUDENT DATA PRIVACY AGREEMENT

NEW HAMPSHIRE

NH-DPA, Research Version 1.0

MANCHESTER SCHOOL DISTRICT SAU 37

and

CAMPUS COMPACT FOR NEW HAMPSHIRE

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, NH 03102 (the "**Local Education Agency**" or "**LEA**") and Campus Compact for New Hampshire, located at 2 Pillsbury Street, Suite 302, Concord, NH 03301 (the "**Provider**").

WHEREAS, the Provider is conducting studies for or on behalf of the LEA to develop, validate or administer predictive tests, administer student aid programs or improve instruction in accordance with 34 CFR § 99.31(a)(6)(i),

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 the duration of the research study. The duration of the research study is outlined in **Exhibit "A".**

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:

Name: Dr. Stephanie Lesperance Title: Chief Strategy Officer

Address: 2 Pillsbury Street, Suite 302, Concord, NH 03301

Phone: 603-223-2302

Email: lesperance@compactnh.org

The designated representative for the LEA for this DPA is:

Stephen P. Cross, CIO
20 Hecker St., Manchester NH 03064
603-624-6300 x162
scross@mansd.org

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

MANCHESTER SCHOOL DISTRICT SAU 37

By: STephen CROSS
STephen CROSS (Apr 23, 2024 17:03 EDT)
Date: 04/22/2024

Printed Name: Stephen P Cross
Title/Position: Chief Information Officer

CAMPUS COMPACT FOR NEW HAMPSHIRE

By:
Date: February 22, 2024

Printed Name: Dr. Stephanie Lesperance
Title/Position: Chief Strategy 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 will be conducting a a study for, or on behalf of, schools, school districts, or postsecondary institutions. Studies can be for the purpose of developing, validating, or administering predictive tests; administering student aid programs; or improving instruction. The parties warrant that the Provider must have access to Student Data to perform the study. 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"**. This Exhibit does not encompass that a student and/or parent provides through written parental consent to the Provider directly pursuant to the study.

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 under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

2. **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.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **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.

5. **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 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. **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.

3. **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.

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 outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

3. **Provider Employee Obligation**. Provider shall conduct the study in a manner that does not permit the personal identification of parents, teachers, and students by anyone other than those with a legitimate need to know to complete the study. 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 agrees to conduct the study so as not to identify students, teachers, or their parents. Provider agrees to take steps to maintain the confidentiality of the Student Data at all stages of the study, including within the final report, by using appropriate disclosure avoidance techniques. 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. Except for Subprocessors, Provider agrees 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.

6. **Disposition of Data**. Upon termination of the research study, Provider shall dispose of all Student Data obtained under the Service Agreement, within sixty (60) days of the date of termination. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified. 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.

8. **Publication**. The Provider must provide the LEA with one electronic copy and at least one paper copy of the final versions of all approved reports and other documents associated with the project. The Provider may not distribute and publish research results and other products of its research until it provides the LEA in advance with a thirty (30) day period in which to review each proposed publication in confidence, provided that the scope and purpose of such review will be limited to the identification of Personally Identifiable Information contained in the publication. At the end of the 30-day review period, the Provider will have the right to publish, excluding any Personally Identifiable Information. For the avoidance of doubt, once a work has been reviewed, the content may be disclosed in substantially the same form on multiple occasions without additional review by Provider.

9. **IRB.** If necessary, the Provider agrees to furnish all documentation concerning Institutional Review Board ("IRB") reviews, and to submit required documentation to an IRB or Privacy Board should research protocols change. Provider agrees to submit to the LEA any change in waiver status or conditions for approval of the project by an IRB relating to the work described in the research proposal.

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.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or 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 LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security**. The Provider agrees to utilize 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 shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. 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 seventy-two (72) hours of confirmation of the incident, 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 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 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 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 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. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

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, license agreement, 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 Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice 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. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

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, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

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

Purpose of the research study to be conducted:

Campus Compact for New Hampshire is the lead organization for two United States Department of Education grants – GEAR UP and Statewide Family Engagement Center. Data gathered will utilized for performance measurement and evaluation.

GEAR UP NH: GEAR UP NH's research study is designed to explore postsecondary and post-college outcomes of the project, while evaluating the efficacy of GEAR UP services associated with these outcomes. Central to this research is the unique potential to examine the impact of formative, data-driven services delivered under a model of continuous improvement.

NH Statewide Family Engagement Center (NH•SFEC): NH•SFEC The study will examine early indicators of progress toward intended outcomes; assess the fidelity of program implementation; and explore factors that facilitate or hinder quality implementation. The evaluation will provide findings related to program quality and impact for all students enrolled in schools or programs implementing the NH•SFEC curriculum. The focus of the evaluation will include:

- National Network of Partnership Schools (NNPS)/Epstein-aligned NH•SFEC curriculum on students
- Descriptive evidence of the impact of the NNPS/Epstein-aligned NH•SFEC curriculum on school staff, and parent outcomes in the regional sites (Manchester, North Country)
- Descriptive evidence of the impact of Family Villages on parent skills, knowledge, and confidence in working with schools and community partners to remove barriers for their children
- Formative feedback on implementation.

Scope of the proposed research study:

***GEAR UP NH*:** Cohort of students in 5th, 6th and 7th grades at the following schools: Berlin Middle School, Claremont Middle School, Franklin Middle School, Henry J McLaughlin Middle School, Henry Wilson Memorial School, Hillside Middle School, Laconia Middle School, Lisbon Regional School (Middle), Middle School at Parkside, Newport Middle School, Pennichuck Middle School, Pittsfield Middle School, Somersworth Middle School, Southside Middle School, Stewartstown Community School

(NH•SFEC): Students and families in the schools across NH with pilot regions of Manchester and northern New Hampshire from birth to postsecondary.

Duration of the research study:

GEAR UP NH: July 2024 through October 2031

(NH•SFEC): July 2024 through September 30 2027

Methodology of the research study:

GEAR UP NH: Student and family surveys will be administered annually to obtain information about perceptions and expectations about GEAR UP, the students' future academic goals, and where they are on their path toward achieving their postsecondary goals. Similarly, an annual school staff survey, rooted in the college-going culture rubric, will be administered to all staff in GEAR UP schools to obtain information about their perceptions regarding the teacher's role in supporting students' postsecondary educational goals. This combined survey data, when coupled with academic data, will provide a holistic picture of student and school progress, thereby aiding in periodic assessments and refinement of the services and activities.
The following quantitative Research Questions will focus on formative and summative evaluations and an embedded research study, all geared towards a holistic view of student achievement. This approach, combined with GEAR UP NH's plan to implement targeted, datadriven services, will aim to provide a rigorous evaluation of GEAR UP NH.
GEAR UP NH Quantitative Research Questions:
1. Formative Evaluation: What is the annual effect of targeted services on increasing academic readiness as measured by end-of-grade assessments in middle school?
2. Formative Evaluation: What is the annual effect of targeted services on increasing academic success as measured by GPA in high school?
3. Summative Evaluation: What is the effect of enrollment in dual enrollment courses on 60 a. subsequent postsecondary enrollment? b. postsecondary persistence?
4. Summative Evaluation: What is the relationship between the number of hours spent in GEAR UP activities and
a. subsequent postsecondary enrollment?
b. postsecondary persistence?
5. Research Study: What is the relationship between access to the GEAR UP NH scholarship and postsecondary enrollment?

(NH•SFEC):
The evaluation methodology will measure parent knowledge, skills, and attitudes related to engaging with the school using a project-designed survey administered in the fall and spring of years 2-5. The survey will include items aligned to Epstein's framework for family engagement, which include understanding, awareness, and confidence related to parenting & child development; communication with school staff; volunteering at school; supporting learning at home; providing input into school policies; and accessing community resources (survey to measure school staff (i.e., leaders and teachers) knowledge, skills, and attitudes related to engaging with parents, aligned to Epstein's framework for family engagement, which include understanding families' background and views of their children; increased diversity and use of communications with families; readiness to involve families in new ways

We will use end-of-year (2027, Y5) and prior-year attendance data (2026, Y4) for students in grades K-12 assigned to treatment and control schools in Year 5. Bellwether will measure attendance using both a continuous variable indicating the number of days a student was absent during one school year as well as a dichotomous variable indicating whether a student was chronically absent (i.e., missing 10% of school days for any reason [USDE]). Academic Achievement (RQ2). We will use student-level state standardized test score data for 2025-26 (Y4, baseline) and 2026-27 (Y5, outcome). NH's state assessment measures success with state standards and include assessments in mathematics and ELA (grades 3-8). Data include the student's scale scores, which are measured as continuous variables.

(NH•SFEC):
1.Do students enrolled in schools participating in the NH•SFEC curricula pilot (NNPS) have higher overall attendance and lower chronic absenteeism relative to a matched comparison group of students from non-

participating schools? Do program impacts differ for students in rural versus urban areas? For students in different age bands (elem., middle, hs)
2. QED. Do students enrolled in schools participating in the NH•SFEC curricula pilot (NNPS) have higher ELA and math achievement relative to a matched comparison group of students from non-participating schools? Do program impacts differ for students attending schools in rural versus urban areas? For students in different age bands (elementary, middle)
3.Descriptive. Do parents participating in the NH•SFEC curricula pilot have improved knowledge, attitudes, and behaviors related to engaging with the school to support their child's academic and developmental needs compared to baseline?
4. Descriptive. Do school staff participating in the NH•SFEC curricula pilot have improved knowledge, attitudes, and behaviors related to engaging with parents to meet the academic and developmental needs of their children compared to baseline?
5. Descriptive. Do parents participating in NH•SFEC Parent Nation have improved knowledge, attitudes, and behaviors—including increased confidence and voice—related to their own abilities to identify and remove barriers that support their children's development?
6. Does NH•SFEC implement Parent Nation as intended? What factors facilitate or hinder quality implementation?
7. Does NH•SFEC implement the NNPS curricula pilot as intended? What factors facilitate or hinder quality implementation?
8. Is NH•SFEC support for the SEA's creation of a statewide infrastructure for meaningful parent engagement implemented as intended? What factors facilitate/hinder quality implementation?
9. How do parents and SEA, LEA, school, and CBO staff perceive the quality and effectiveness of NH•SFEC programming and support?

How the PII will be used/disclosed:

For all projects, PII will be used for research and analysis purposes but not published or released outside of our data collection system – Compass which utilizes Azure. Azure has NIST SP 800-53 Rev. 4 Azure regulatory compliance built-in initiative.

Any PII will be redacted when sharing with outside evaluators for analysis purposes and data will be aggregated whenever possible.

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	X
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	X
	Student class attendance data	X
Communications	Online communications captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	X
Demographics	Date of Birth	X
	Place of Birth	X
	Gender	X
	Ethnicity or race	X
	Language information (native, or primary language spoken by student)	X
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	X
	Specific curriculum programs	X
	Year of graduation	X
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	X
	Email	X
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	X

Category of Data	Elements	Check if Used by Your System
Parent/Guardian Name	First and/or Last	X
Schedule	Student scheduled courses	X
	Teacher names	X
Special Indicator	English language learner information	X
	Low income status	X
	Medical alerts/ health data	X
	Student disability information	X
	Specialized education services (IEP or 504)	X
	Living situations (homeless/foster care)	X
	Other indicator information-Please specify:	
Student Contact Information	Address	X
	Email	X
	Phone	X
Student Identifiers	Local (School district) ID number	X
	State ID number	X
	Provider/App assigned student ID number	X
	Student app username	X
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	X
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures, etc.	X
	Other student work data -Please specify:	X
Transcript	Student course grades	X
	Student course data	X
	Student course grades/ performance scores	X
	Other transcript data - Please specify:	X
Transportation	Student bus assignment	X

Category of Data	Elements	Check if Used by Your System
	Student pick up and/or drop off location	X
	Student bus card ID number	X
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

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 organizations conducting studies for, or on behalf of, schools, school districts, or postsecondary institutions. Studies can be for the purpose of developing, validating, or administering predictive tests; administering student aid programs; or improving instruction.

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.

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 includes Meta Data. 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. Student Data shall not constitute information that a student and/or parent provides through written parental consent directly to the Provider pursuant to the study.

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."

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 "E"

GENERAL OFFER OF PRIVACY TERMS

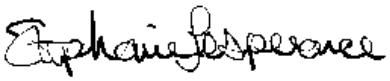
1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and **Manchester School District SAU 37** ("Originating LEA") which is dated March 28, 2024, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form.

Subscribing LEAs should send the signed Exhibit "E" to Provider at the following email address:

lesperance@compactnh.org.

CAMPUS COMPACT FOR NEW HAMPSHIRE



BY: Date: March 28, 2024

Printed Name: Dr. Stephanie Lesperance Title/Position: Chief Strategy Officer

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the **Manchester School District SAU 37** and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

Subscribing LEA: (School District Name): _____

BY: _____Date:_____

Printed Name: _____ Title/Position: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

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

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	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
	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".**

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,…"
3. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
4. 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) inform, influence, or enable marketing,

advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, 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.

5. The Provider agrees to the following privacy and security standards. 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 or Teacher Data in accordance with NIST SP 800-88 Revision 1;

    (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;

    (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;

    (15) Control access to media containing Student Data or Teacher 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 and Teacher 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.

Alternatively, the Provider agrees to comply with one of the following standards: (1) NIST SP 800-171 rev 2, Basic and Derived Requirements; (2) NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher; (3) FedRAMP (Federal Risk and Authorization Management Program); (4) ISO/IEC 27001:2013; (5) Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher; (6) AICPA System and Organization Controls (SOC) 2, Type 2; and (7) Payment Card Industry Data Security Standard (PCI DSS), v3.2.1. The Provider will provide to the LEA on an annual basis and upon written request demonstration of successful certification of these alternative standards in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (PATO) issued by the FedRAMP Joint Authorization Board (JAB).

6. 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:

    i. The estimated number of students and teachers affected by the breach, if any.

7. 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 "I"

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

ResearchDPA_Manchester - CCNH

Final Audit Report 2024-04-23

Created:	2024-03-28
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA8knjuWwS-BeIOSFJftTq2my3pdp8i6dM

"ResearchDPA_Manchester - CCNH" History

Document created by Ramah Hawley (rhawley@tec-coop.org)
2024-03-28 - 2:55:54 PM GMT- IP address: 108.35.203.7

Document emailed to STEVE CROSS (scross@mansd.org) for signature
2024-03-28 - 2:55:59 PM GMT

Email viewed by STEVE CROSS (scross@mansd.org)
2024-04-23 - 9:02:28 PM GMT- IP address: 216.107.231.34

Signer STEVE CROSS (scross@mansd.org) entered name at signing as STephen CROSS
2024-04-23 - 9:03:23 PM GMT- IP address: 216.107.231.34

Document e-signed by STephen CROSS (scross@mansd.org)
Signature Date: 2024-04-23 - 9:03:25 PM GMT - Time Source: server- IP address: 216.107.231.34

Agreement completed.
2024-04-23 - 9:03:25 PM GMT