STANDARD STUDENT DATA PRIVACY AGREEMENT

MASSACHUSETTS, NEW HAMPSHIRE AND RHODE ISLAND

MA-NH-RI-DPA, Modified Version 1.0

DANVERS PUBLIC SCHOOLS

and

EDUCATIONSUPERHIGHWAY

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: Danvers Public Schools, located 64 Cabot Road, Danvers, MA 01923 (the "**Local Education Agency**" or "**LEA**") and EducationSuperHighway, located at 6 Presidio Terrace, San Francisco, CA 94118 (the "**Provider**" and together with the LEA, the "**Parties**" and each, a "**Party**").

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). Provider will receive information from both the LEA and each ISP (as hereinafter defined) and facilitate an exchange of information between such parties in furtherance of the Purpose.

WHEREAS, Provider will receive information from both the LEA and each ISP and facilitate an exchange of information between such parties in furtherance of the Purpose.

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 **<u>Exhibit "G"</u>** are hereby incorporated by reference into this DPA in their entirety.

   □If Checked, the Provider, has signed **<u>Exhibit "E"</u>** 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 **<u>Exhibit "A".</u>**

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **<u>Exhibit "A"</u>** (the "**Services**").

6. **<u>Notices</u>**. 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:

Evan Marwell, CEO
EducationSuperHighway
(415) 425-8610
evan@educationsuperhighway.org

The designated representative for the LEA for this DPA is:

James K. Sullivan, CETL, Director of Technology & Technology Integration
Danvers Public Schools
(978) 777-8925 x2259
sullivan@danvers.org

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

DANVERS PUBLIC SCHOOLS

By: James K. Sullivan
James K. Sullivan (Apr 21, 2021 11:26 EDT)
Date: 4/21/2021

Printed Name: James K. Sullivan
Title/Position: Director of Technology

EDUCATIONSUPERHIGHWAY

By: Evan C. MArwell
Evan C. MArwell (Apr 21, 2021 07:04 PDT)
Date: 4/21/21

Printed Name: Evan Marwell
Title/Position: CEO

<u>STANDARD CLAUSES</u>
Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **<u>Purpose of DPA</u>**. 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 study for, or on behalf of, schools, school districts, or postsecondary institutions. Provider is interested in working with a LEA to help facilitate remote learning, in connection with the implementation of a program that provides broadband services (the "**ISP Services**") through various broadband providers (each an "**ISP**") to certain eligible households ("**End Users**") to support remote working and learning solutions within [DESCRIBE SPECIFIC COVERED TERRITORY] (the "**Covered Territory**"), free of charges to the End Users (the "**Purpose**"). 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. Learning which homes ISPs are able to service can be accomplished efficiently through the LEA providing addresses of students to the LEA. The LEA will then share the addresses with Provider for the sole purpose of determining whether the ISP can provide ISP Services to such address.
2.
3. **<u>Student Data to Be Provided</u>**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **<u>Exhibit "B"</u>**. This Exhibit does not encompass that a student and/or parent provides through written parental consent to the Provider directly pursuant to the study.

4. **<u>DPA Definitions</u>**. The definition of terms used in this DPA is found in **<u>Exhibit "C"</u>.** 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. **<u>Student Data Property of LEA</u>**. 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. **<u>Parent Access</u>**. 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, and it shall only take place after prior notification of the LEA. 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. The prior sentence does prohibit the Provider from transferring addresses to Broadband providers pursuant to the Services.

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. This requirement does not prevent the Provider from publishing aggregate summary statistics by themselves.

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: MUTUAL DUTIES

1. **Data Confidentiality**.
   a. The parties hereto shall protect and safeguard the confidentiality of all Confidential Information, using the same degree of care to safeguard and avoid disclosure of any of the Confidential Information obtained hereunder as it would use with respect to its own Confidential Information or proprietary information, but in any case using no less than a reasonable degree of care.
   b. The parties shall: (i) carefully restrict access to Confidential Information solely to those employees, contractors, and third parties who have a need to know such Confidential Information as reasonably required for the execution of the parties' duties; and (ii) advise such persons of the proprietary and/or confidential nature of the Confidential Information and of the obligations set forth in this Agreement. Absent the prior written approval of the other Party, each Party shall not publish, copy, summarize, use for the Party's own benefit in any manner, otherwise disclose to others, or permit the use by others for their benefit or to the detriment of the other Party, any Confidential Information.

2. **Data Disclosure**. Neither Party shall disclose the Data Set or Confidential Information contained therein to any entity other than ISPs or the LEA that provided the Data Set or Confidential Information to the LEA, except that the LEA may respond to and provide information in response to a public records request in accordance with the law.

3. **Permitted Uses and Disclosures**.
   a. Provider may disclose the Data Set to the ISP and use the Data Set in connection with the Purpose. The LEA may disclose Confidential Information related to the ISP solely in connection with the Purpose described in this Agreement.
   b. Neither Provider nor the LEA shall use the Data Set for any purpose that is not explicitly authorized by this Agreement. This restriction includes, but is not limited to, any use by Provider for marketing or solicitation purposes that involves Provider contacting an address contained in the Data Set or an individual residing at such address.

ARTICLE VI: 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. **Notification**. Each party shall report to the other any use or disclosure of the Data Set or Confidential Information not provided for by this Agreement.

3. **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.

4. **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.

5. **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 Parties, each party shall provide notification to the other party within twenty-four (24) hours of discovering the violation, 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. Each Party 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 Party and as it becomes available:

      i. The name and contact information of the reporting LEA or Provider 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) Each Party 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) Each Party 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 the other party, 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 VII: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **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 VIII: 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/Destruction of Information**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6. Provider will only hold Confidential Information provided under this Agreement only as long as necessary to meet the purposes of this Agreement. Provider agrees to destroy all Confidential Information as soon as it is no longer needed for purposes of this Agreement. The LEA agrees to promptly destroy any and all records related to Confidential Information received from or related to an ISP upon written request from Provider.

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:
K-12 Bridge to Broadband is an initiative to ensure that all students are connected to broadband to support remote working and learning solutions. The purpose of this study is to (1) provide participating LEAs with an accurate understanding of which households are unconnected and the ISPs that can serve those households and (2) leverage data aggregated at the LEA level to inform local, state, and federal policy-makers of the connectivity gap and related trends.

Scope of the proposed research study:
The scope of the study is national and will enroll LEAs seeking to address home broadband access challenges for their students. EducationSuperHighway will facilitate a data exchange between participating LEAs and ISPs to determine household- and student-level connectivity status. The data exchanged between all entities will be limited to address data, and data on each ISP’s capability to service such address. LEAs may elect to participate in the data exchange as a single event or as an ongoing exercise (e.g. once a year when enrollment data is refreshed).

Duration of the research study:
The study will run until June 30th, 2023 (with the potential to extend based on LEA requirements and demands). The results produced by this study will support ongoing efforts by LEAs to address the digital divide for their families. LEAs or ISPs may refresh data to reflect the most up-to-date status of household connectivity.

The anticipated long-term impacts of the COVID-19 pandemic and fundamental changes to how educators deliver learning to students will make this data vital to LEA operations for the foreseeable future. The study’s time frame allows for adequate trend data to be collected and reported on to inform policy-makers of progress and the remaining need.

Methodology of the research study:
Each participating LEA will provide anonymized address data for all student households to EducationSuperHighway. EducationSuperHighway will share anonymized address data with ISPs that have a service territory covering a significant percentage of the addresses shared.

For each address shared, the ISP will indicate one of three statuses: (1) household is a current subscriber, (2) household is not a current subscriber but service is available at the address, or (3) service is not available at the address.

EducationSuperHighway will conduct an analysis of all ISP responses to identify: (1) number of students with a broadband connection, (2) number of students without a broadband connection and service is available, (3) number of students without a broadband connection and service is not available. For category (2), the study will also provide the ISP(s) that can serve each address.

How the PII will be used/disclosed:
EducationSuperHighway will collect address data only from participating LEAs. This data will be disclosed by ESH to ISPs, in order to collect subscriber and serviceability data for each household.

Data generated by the study will be aggregated at the LEA level. EducationSuperHighway will maintain aggregated data beyond the duration of the study for reporting and advocacy purposes.

All data collected is stored on EducationSuperHighway's secure platform.

- EducationSuperHighway's infrastructure runs in the cloud using third party vendors that maintain security standards and compliance certifications, including SOC 2, ISO 27001, Federal Risk and Authorization Management Program (FedRAMP), PCI-DSS, HIPAA/HITECH, FedRAMP, GDPR, FIPS 140-2, and NIST 800-171. Learn more here.
- Data and web content are always encrypted-in-transit, both within internal systems and to or from external systems. This encryption will be performed using AES-128, AES-256, or better recognized by the broader security community.
- Data is always encrypted-at-rest, including file-level encryption or full disk-level encryption, usually simultaneously (using AES-128, AES-256, or better).
- HTTPS is enabled and required for all web-based services, using TLS 1.1 or higher.
- All data access points and interfaces require both authentication and authorization, limiting access to only those parties who have a legitimate need for the provision of our services. Where possible, this will additionally require multi-factor authentication.
- Data is always securely destroyed using data deletion techniques outlined in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data. Learn more here.
- We review all changes made to the source code underlying our products and services for potential flaws in logic, security, or otherwise. All changes are automatically scanned for known security vulnerabilities.
- System events, including but not limited to automatic systems operations, data access, and administrative actions, are automatically gathered into audit logs which are archived and regularly reviewed.
- Our staff stays current on the latest tools and techniques to enhance our security and privacy practices and adopt them where necessary. All employees sign agreements barring any use of confidential information outside of the scope of their work. We provide security and technology use training to all employees.

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	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	X
	Email	

	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	X
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	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)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	

	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	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

Confidential Information: "Confidential Information" means any information shared by either Party that is not publicly available or is otherwise protected from disclosure by federal or state law, and includes which should reasonably be recognized as confidential information, including, without limitation, (i) personally identifiable information from an education record of a student, as those terms are defined in 34 C.F.R. § 99.3. Confidential Information includes student unique identifier, demographic or other descriptive elements, and addresses contained in the Data Set and (ii) information relating to an ISP's capability to provide services at various addresses, any information relating to ISP's subscribers or end users, including the names, addresses, e-mail addresses and telephone numbers of all subscribers or end users and prospective subscribers or end users to any product or service offered by any ISP, including all lists or records of such information, all technical information relating to a ISP's services, network configuration and capabilities and all other proprietary information relating to the operations of any ISP which was disclosed or provided to the LEA or became known to the parties through its relationship with the other Party.

Data Set: "Data Set" shall refer to one or more sets of Confidential Information containing addresses provided to Provider from the LEA under this Agreement.

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.

ISP: means a company or other entity that provides internet service to residences in the geographic area in which students of District live.

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.

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

(To be completed at a later date)

[**Insert Name of 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 **DANVERS PUBLIC SCHOOLS** ("Originating LEA") which is dated 4/21/2021______________, 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:

____.

EDUCATIONSUPERHIGHWAY

BY: Evan C. MArwell
Evan C. MArwell (Apr 21, 2021 07:04 PDT) Date: 4/21/21

Printed Name: Evan Marwell Title/Position: CEO

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 **DANVERS PUBLIC SCHOOLS** and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VIII, 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"
Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; 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 Massachusetts;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

EXHIBIT "G"
Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 et. seq.; 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 Rhode Island;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
4. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
5. In the case of a data breach, as a part of the security breach notification outlined in Article VI, Section 5(1), the Provider agrees to provide the following additional information:

   i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:

      1. The credit reporting agencies
      2. Remediation service providers
      3. The attorney general

   ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

   iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

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" and delete "or stated in the Service Agreement."
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) 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.

7. 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).

8. In the case of a data breach, as a part of the security breach notification outlined in Article VI, Section 5(1), the Provider agrees to provide the following additional information:

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

9. 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)	
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Teacher app username	
	Teacher app passwords	
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	

	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	

ESH_Danvers

Final Audit Report 2021-04-21

Created:	2021-04-21
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAC7O1k5bTeotGENcxUaBdm52gXvGyzWz-

"ESH_Danvers" History

Document created by Ramah Hawley (rhawley@tec-coop.org)
2021-04-21 - 10:44:16 AM GMT- IP address: 100.1.115.187

Document emailed to Evan C. MArwell (evan@educationsuperhighway.org) for signature
2021-04-21 - 10:47:32 AM GMT

Email viewed by Evan C. MArwell (evan@educationsuperhighway.org)
2021-04-21 - 2:03:21 PM GMT- IP address: 76.102.230.70

Document e-signed by Evan C. MArwell (evan@educationsuperhighway.org)
Signature Date: 2021-04-21 - 2:04:27 PM GMT - Time Source: server- IP address: 76.102.230.70

Document emailed to James K. Sullivan (sullivan@danvers.org) for signature
2021-04-21 - 2:04:29 PM GMT

Email viewed by James K. Sullivan (sullivan@danvers.org)
2021-04-21 - 2:04:51 PM GMT- IP address: 74.125.212.15

Document e-signed by James K. Sullivan (sullivan@danvers.org)
Signature Date: 2021-04-21 - 3:26:23 PM GMT - Time Source: server- IP address: 50.232.239.238

Agreement completed.
2021-04-21 - 3:26:23 PM GMT