

STANDARD STUDENT DATA PRIVACY AGREEMENT

**MASSACHUSETTS, MAINE, ILLINOIS, IOWA, MISSOURI, NEBRASKA, NEW HAMPSHIRE,
NEW JERSEY, NEW YORK, OHIO, RHODE ISLAND, TENNESSEE, VERMONT, AND VIRGINIA**

MA-ME-IL-IA-MO-NE-NH-NJ-NY-OH-RI-TN-VT-VA-NDPA, Standard Version 1.0

Frederick County Public Schools

and

MathSpace, Inc.

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: Frederick County Public Schools, located at 1415 Amherst Street, Winchester, VA 22601 USA (the “**Local Education Agency**” or “**LEA**”) and MathSpace, Inc., located at 228 Park Ave. S., #15992, New York, NY 10003 USA (the “**Provider**”).

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

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

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

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

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

The designated representative for the Provider for this DPA is:

Name: ALVIN SAVOY Title: CTO

Address: SUITE 2.111 477 PITT ST, HAYMARKET NSW 2000 AUSTRALIA

Phone: +1 480-630-6425 Email: asavoy@mathspace.com.au

The designated representative for the LEA for this DPA is:

Timothy Grant, Director of IT
1415 Amherst Street, Winchester, VA 22601
540-662-3888 grantt@fcpsk12.net

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

Frederick County Public Schools

By:  Date: 10/27/2025
Timothy Grant (Oct 27, 2025 14:45:50 EDT)

Printed Name: Timothy Grant Title/Position: Director of Technology

MathSpace, Inc.

By:  Date: 10/27/2025

Printed Name: Mohamad Jebara Title/Position: CEO

STANDARD CLAUSES

Version 3.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit “C”**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **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. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

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 require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, 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. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."
7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** 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

MathSpace, an adaptive online learning platform.

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.	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
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	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
	Student grade level	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
Schedule	Student scheduled courses	
	Teacher names	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
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	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
	Student app username	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
	Student app passwords	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Student Name	First and/or Last	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
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.	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
	Student course grades/ performance scores	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

Category of Data	Elements	Check if Used by Your System
	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.	



Data elements collected are indicated above

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 provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

Student Generated Content: The term “student-generated content” means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

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

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

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians, that is descriptive of the student including, but not limited to, information in the student’s educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline

records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data 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.

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 “F”
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

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

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.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

EXHIBIT "G"
Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; 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 Maine;

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. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
 - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
 - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
 - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

EXHIBIT “G”
Illinois

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Illinois. Specifically, those laws are to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act (“LRA”), 50 ILCS 205; 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 Illinois;

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

1. Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be replaced with: “This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. The Exhibit E General Offer will expire three (3) years from the date the original DPA was signed.”
2. Replace Notices with: “Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.”
3. In Article II, Section 1, add: “Further clarifying, in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.”
4. In Article II, Section 2, replace “forty-five (45)” with “five (5)”. Add the following sentence: “In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA.”

5. In Article II, Section 4, replace it with the following: “In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.”
6. In Article II, Section 5, add: “By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).”
7. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
8. In Article IV, Section 6, replace the whole section with:

The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

9. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
10. In Article IV, Section 7, add “renting,” after “using.”

11. In Article V, Section 1 Data Storage: Illinois requires all Student Data to be stored within the United States, Canada, United Kingdom and/or the European Union.
12. In Article V, Section 4, add the following: “‘Security Breach’ does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.”
13. In Article V, Section 4(1) add the following:
 - vi. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and
 - vii. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.
14. In Article V, Section 4, add a section (6) which states:

In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

 - a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;
 - b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;
 - c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA

as a result of the security breach; and

 - d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.
15. Replace Article VII, Section 1 with: “In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate.”
16. In Exhibit C, add to the definition of Student Data, the following: “Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school

student records", "student temporary record" or "student permanent record" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA."

17. The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E:
"The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first."
18. The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.
19. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider's products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.
20. **Student and Parent Access.** Access by students or parents/guardians to the Provider's programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.
21. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.
22. The Provider will not collect social security numbers.

EXHIBIT “G”
Iowa

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Iowa. Specifically, those laws are Iowa Code §§ 22; Iowa Code §§ 715C, 281 I.A.C. 12.3(4); 41; 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 Iowa;

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. In Article V, Section 1 Data Storage: Iowa does not require all Student Data to be stored within the United States.
4. In Exhibit “C” add to the definition of “Student Data” significant information on progress and growth, experiences, interests, aptitudes, attitudes, abilities, part-time employment, and future plans.

EXHIBIT “G”

Missouri

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Missouri. Specifically, those laws are Sections 162.1475 and 407.1500 RSMo; 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 Missouri;

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. In Article V, Section 1 Data Storage: Missouri does not require data to be stored within the United States.
4. Replace Article V, Section 4(1) with the following:
 - a. In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student’s family member, Provider shall notify LEA within seventy-two (72) hours. The notice shall include:
 - i. Details of the incident, including when it occurred and when it was discovered;
 - ii. The type of personal information that was obtained as a result of the breach; and
 - iii. The contact person for Provider who has more information about the incident.
 - b. “*Breach*” shall mean the unauthorized access to or unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person employed by or contracted with, or an agent of, Provider is not a breach provided that the personal information is not used in violation of applicable Federal or Missouri law, or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.
 - c. “*Personal information*” is the first name or initial and last name of a student or a family member of a student in combination with any one or more of the following data items that relate to the student or a family member of the student if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology such that the name or data elements are unreadable or unusable:
 - i. Social Security Number;
 - ii. Driver’s license number or other unique identification number created or collected by a government body;
 - iii. Financial account information, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - iv. Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - v. Medical information; or
 - vi. Health insurance information.

EXHIBIT “G”
Nebraska

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Nebraska. Specifically, those laws are Neb. Rev. Stat. Secs. 79-2,104; 79-2,153 to 79-2,155; 79-2, 539; 87-801 to 87-808; and 92 NAC 6; 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 Nebraska;

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

1. In Article II, Section 5, add, “Specifically, any written agreement with a Subprocessor will: (1) prohibit the Subprocessor from using Student Data any purpose other than providing the contracted service to or on behalf of the Provider; (2) prohibit the Subprocessor from disclosing any Student Data provided by the Provider with subsequent third parties; (3) and requires the Subprocessor to implement and maintain reasonable security procedures and practices.”
2. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
3. In Article IV, Section 4, replace: “Provider will not Sell Student Data to any third party” with “Provider will not Sell or rent Student Data to any third party.
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Nebraska does not require data to be stored within the United States.

EXHIBIT "G"

Ohio

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Ohio. Specifically, those laws are R.C. §§ 3319.32-3319.327, R.C. §§ 1349.17-19, Rule 3301-51-04; 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 Ohio;

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. In Article IV, Section 3, add: "The Provider will restrict unauthorized access by Provider's employees or contractors not providing services under the Service Agreement or DPA and its employees or contractors will only access Student Data as necessary to fulfill their official duties."
3. In Article IV, Section 6, replace "Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice," with "Upon termination of this DPA, unless the LEA provides notice that renewal of the contract is reasonably anticipated, within ninety (90) days of the expiration of the contract, Provider shall destroy or return Student Data to the LEA."
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Ohio does not require data to be stored within the United States.
6. Provider will not access or monitor any of the following:
 - a. Location-tracking features of a school-issued device;
 - b. Audio or visual receiving, transmitting or recording features of a school-issued device;
 - c. Student interactions with a school-issued device, including, but not limited to, keystrokes and web-browsing activity

Notwithstanding the above, if the Provider has provided written notice to the LEA that it engages in this collection of the above information, which must be provided in the Service Agreement, and the LEA has provided written confirmation that the Provider can collect this information pursuant to its general monitoring, then the Provider may access or monitor the listed information.

EXHIBIT "G"
New Jersey

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Jersey. Specifically, those laws are N.J. Stat. § 56:8-166.4 et seq.; N.J. Stat. § 18A:36-19; N.J. Stat. § 18A:36-19a; N.J. Stat. § 18A:36-35; N.J. Admin Code § 6A:16-7.9; N.J. Admin. Code § 6A:32-2.1; N.J. Admin. Code § 6A:32-7 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 New Jersey;

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 will not disclose on its web site any personally identifiable information about a student, including, but not limited to student names, student photos, student addresses, student e-mail addresses, student phone numbers, and locations and times of class trips.
4. The Provider will not process Student Data in violation of State and federal laws that prohibit unlawful discrimination.
5. The Provider will not conduct processing that presents a heightened risk of harm to students without conducting and documenting a data protection assessment of each of its processing activities that involve Student Data.
6. In Article V, Section 1 Data Storage: New Jersey does not require data to be stored within the United States.
7. Add to the definition in Exhibit "C" of Student Data: "The location and times of class trips."

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. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
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. 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"
Tennessee

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Tennessee. Specifically, those laws are T.C.A. §§ 10-7-503 *et. seq.*, T.C.A. § 47-18-2107, T.C.A. § 49-1-701 *et. seq.*, T.C.A. § 49-2-211, T.C.A. § 49-6-902, § 49-6-3001, T.C.A. §§ 49-50-1501 *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 Tennessee;

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. In Article V, Section 1 Data Storage: Tennessee does not require data to be stored within the United States.
4. The Provider agrees that it will not collect any individual student biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking.
5. The Provider agrees that it will not collect individual student data on:
 - a. Political affiliation;
 - b. Religion;
 - c. Voting history; and
 - d. Firearms ownership

EXHIBIT "G"

Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; 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 Vermont;

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. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT “G”
Virginia

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Virginia. Specifically, those laws are Code of Virginia § 22.1-289.01 and Virginia Code § 2.2-5514(c); 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 Virginia;

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. In Article V, Section 1 Data Storage: Virginia does not require data to be stored within the United States.
4. In Article V, Section 4, add: In order to ensure the LEA’s ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within twenty-four (24) hours, where the Provider reasonably expects or confirms Student Data may have been disclosed in a data breach.

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 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.
- 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.
- 10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

EXHIBIT "I" – TEACHER DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
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	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
	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	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
	Teacher app username	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
	Teacher app passwords	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
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	

Exhibit "G"

New York

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those laws are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into these additional 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 York;

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

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.
3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.
4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.
5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the DPA to “Student Data” shall be amended to include and state, “Student Data and APPR Data.”
7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply with the LEA’s Data Privacy and Security Policy. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor’s Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.
8. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider’s employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.
10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider’s certifying that it and it’s subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any assurance of discontinuation, which will control in the case of a conflict.

Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a **"Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D"**, or, with reasonable notice to the Provider, other form of its choosing. 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"**.

11. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."
12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
13. To replace Article V, Section 2 (Audits) to state: No more than once a year or following an 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 or its designee(s) 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 or its designee(s) 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.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 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; and
 - vi. The number of records affected, if known; and
 - vii. A description of the investigation undertaken so far; and
 - viii. The name of a point of contact for Provider.
- (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. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.
- (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.
- (6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.

- “Provider” is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit “C” the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure:** The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
- **Participating School District:** As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational programs.
-

Exhibit “J”
LEA Documents

New York LEAs will provide links to their Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy, and supplemental information for this service agreement in their Exhibit Es.

Exhibit "K"
Provider Security Policy

Provider's Data Security and Privacy Plan can be accessed at
REFER TO ATTACHED DOCUMENT



Mathspace Data Security & Privacy Plan - NIST CSF v1.1

1. Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract

Framework Alignment

Mathspace implements data security and privacy contract requirements over the life of the Contract in alignment with the **NIST Cybersecurity Framework v1.1**, through a combination of technical, administrative, and organizational controls.

Governance & Oversight

- Formal Information Security Program managed by CTO (designated security officer), reviewed by leadership.
- Dedicated privacy officer ensures compliance with privacy regulations.
- Agreement to district Data Privacy Addendums and FERPA obligations.

Contract Compliance & Lifecycle Integration

- Contractual obligations embedded across Mathspace teams.
- Full lifecycle compliance with security architecture requirements.

Technical & Administrative Controls

- Encryption: TLS 1.2+ in transit, AES-256 at rest with AWS KMS.
- Access Control: RBAC, MFA, least-privilege enforced.
- Logging: Activity logs retained for 90 days and available upon request.

Monitoring, Auditing & Reporting

- Continuous monitoring with AWS GuardDuty, Inspector, etc.
- Monthly vulnerability scans and annual penetration tests.
- Notification of incidents within 72 hours, including RCA and CAP.

Data Retention & Disposal

- Obfuscation of personal data after 90 days of deactivation.
- Backups deleted after 3 months.

- Secure deletion of all data at contract end or data processing conclusion.

Change Management & Business Continuity

- Formal change management process in place.
- Business Continuity & Disaster Recovery tested regularly (RTO/RPO of 24h).

Training & Awareness

- Security & privacy training at onboarding and annually.
- Refreshed regularly to address new threats.

2. Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII

Mathspace implements a multi-layered approach to protect personally identifiable information (PII) using administrative, operational, and technical safeguards aligned.

Administrative Safeguards

- Mathspace enforces role-based access controls, security training, formalised policies and procedures, and background checks for staff. Data protection policies cover access management, vendor oversight, data handling, and privacy compliance.

Operational Safeguards

- Incident response planning, data classification, regular risk assessments, and business continuity planning form the operational core of Mathspace's data protection program. Vendor risk is assessed periodically, and privacy impact assessments are conducted when required.

Technical Safeguards

- Data is encrypted in transit (TLS 1.2 or higher) and at rest using AES-256. Access is protected by multi-factor authentication and least privilege principles. All systems are monitored for anomalous activity, and vulnerability scans and penetration tests are performed regularly. Data is hosted securely in AWS, with segregation by environment (prod, staging, dev) and regular automated backups.

3. Address the training received by your employees and any subcontractors on the federal and state laws that govern the confidentiality of PII

All Mathspace employees and subcontractors undergo training on data protection and privacy obligations, including federal and state laws governing the confidentiality of personally identifiable information (PII). This training is delivered as part of the onboarding process and is refreshed annually. It includes specific instruction on compliance with the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and applicable state-level student data privacy laws. The training

emphasizes secure handling of PII, breach prevention, and the importance of maintaining confidentiality when accessing or processing sensitive information.

4. Outline contracting processes that ensure employees and subcontractors are bound by the Contract requirements

Mathspace ensures that both employees and subcontractors are contractually bound to uphold the same security, privacy, and confidentiality obligations required by our customer agreements. All employees are subject to contractual agreements that include confidentiality clauses and acknowledgment of our internal security policies. Subcontractors are engaged through contracts that mandate compliance with Mathspace's data protection requirements, including adherence to applicable privacy laws and the NIST Cybersecurity Framework. These agreements are reviewed and enforced through established vendor management and procurement processes.

5. Specify how you will manage data-security and privacy incidents that implicate PII, including breach identification and reporting to the EA

Mathspace follows the NIST Cybersecurity Framework v1.1 and has a defined Incident Response Plan (IRP) to manage data-security and privacy incidents involving personally identifiable information (PII). In the event of a suspected or confirmed breach, we promptly initiate incident identification, containment, eradication, and recovery procedures.

Incidents involving PII are assessed for impact and severity. Once verified, we notify affected parties and the relevant Education Agency without undue delay, in accordance with applicable laws and contractual obligations. Our response includes a description of the nature of the breach, the type of data affected, mitigation steps taken, and guidance for impacted individuals.

Mathspace logs all incidents, conducts post-incident reviews, and implements corrective actions to reduce the likelihood of recurrence.

6. Describe how data will be transitioned to the EA when no longer needed to meet contractual obligations

Upon written request, Mathspace will export customer data in a structured, commonly used, and machine-readable format (e.g., CSV or JSON) and provide it to the EA through a secure transfer method. Once confirmation of receipt is obtained from the EA, Mathspace will securely delete all customer data from its systems in accordance with its data retention and deletion policies.

7. Describe your secure destruction practices and how certification will be provided to the EA

Mathspace follows secure destruction practices aligned with the NIST Cybersecurity Framework v1.1 to ensure the protection of sensitive data throughout its lifecycle. When data is no longer required for

operational or legal purposes, it is securely deleted using methods that render the data unrecoverable. This includes cryptographic erasure and the use of secure wipe tools for applicable systems.

For physical media, destruction is managed by third-party vendors certified in secure disposal. Upon request, Mathspace will provide the Education Agency with a certificate of destruction confirming that data or media has been securely and irretrievably destroyed in accordance with policy and contractual obligations.

8. Outline how your data-security and privacy program/practices align with the EA's applicable policies

Mathspace's data security and privacy program is aligned with the NIST Cybersecurity Framework v1.1 and is structured to support the needs and regulatory obligations of Education Agencies (EAs). Our practices cover all five NIST CSF functions: Identify, Protect, Detect, Respond, and Recover, ensuring a comprehensive and proactive approach to cybersecurity.

We maintain strict access controls, encryption of data both in transit and at rest, secure software development practices, and routine vulnerability assessments. Our privacy program aligns with FERPA and other applicable data protection laws, ensuring that student data is collected, stored, and processed responsibly and only for educational purposes.

Regular staff training, vendor risk management, and incident response readiness are core components of our governance. Our policies and controls are reviewed regularly to ensure they remain aligned with EA requirements and evolving threats.

9. Outline how your data-security and privacy program/practices materially align with the NIST CSF v1.1

See framework below.

Exhibit C.1 - NIST CSF Table

To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>.

Asset Management (ID.AM)

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

Sub-category	Mathspace alignment
ID.AM-1 Physical devices and systems are inventoried	All corporate laptops and networking hardware are logged in a central asset register, updated at provisioning and de-provisioning. The register is reviewed quarterly and reconciled with HR exit reports to ensure devices are returned and accounted for.
ID.AM-2 Software platforms and applications are inventoried	Production hosts run an automated agent that reports installed packages to AWS Inspector; findings are exported to the asset register so that both OS and application stacks remain in scope for patching, vulnerability management and licence tracking.
ID.AM-3 Organizational communication and data flows are mapped	Network and data-flow diagrams covering edge (Cloudflare), AWS VPCs, and third-party integrations are maintained in the architecture repository and must be updated as part of the change-management checklist before release.
ID.AM-4 External information systems are catalogued	All cloud and SaaS providers (e.g. AWS, Cloudflare, Clever, Schoology) are listed in the vendor-risk register; the security team reviews contracts and security posture annually and verifies MFA and data-handling commitments.
ID.AM-5 Resources are prioritized by classification, criticality and value	The Information Security Classification Framework labels assets Public, Internal or Confidential. Production databases and backups classed "Confidential" receive AES-256 encryption, point-in-time recovery and an RTO/RPO of 24 h, while lower-tier assets follow standard backup cycles.
ID.AM-6 Cybersecurity roles and responsibilities are established	Asset ownership, least-privilege access and lifecycle tasks are defined in the Security Program. The security team (asset custodians) oversees inventories; Engineering maintains software BOM; Procurement manages supplier reviews; all roles are communicated company-wide.

Overall NCSR Maturity Self-Rating: 4 - Managed

Business Environment (ID.BE)

The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

Sub-category	Mathspace alignment
ID.BE-1 Role in the supply chain is identified and communicated	A dedicated vendor-risk team vets all service providers, enforces security clauses in contracts, and tracks upstream dependencies (AWS, Cloudflare, open-source libraries). Supply-chain risks are reviewed twice a year and MFA is mandatory for all partner access.
ID.BE-2 Position within sector is understood	Mathspace serves the K-12 education sector as a SaaS learning platform. Stakeholders include students, teachers, district administrators, and regulators. Regulatory drivers such as FERPA, COPPA, GDPR and CCPA are documented in policies and customer agreements.
ID.BE-3 Mission, objectives and priorities are established	Company mission is to provide a reliable, secure digital math tutor. Security objectives align with a 99.5 percent availability target, annual risk assessments and senior-management program reviews that drive resource allocation and roadmap decisions.
ID.BE-4 Dependencies and critical functions are mapped	Critical services (content delivery, authentication, roster sync and data storage) are catalogued with their AWS components. The business-continuity plan lists people, processes, technology and cross-region hosting, with daily tested backups and two geographically diverse data centers.
ID.BE-5 Resilience requirements are defined	Resilience targets include a 99.5 percent SLA, RTO 24 h and RPO 24 h. An HA architecture with autoscaling, continuous replication and annual disaster-recovery tests ensures these requirements are met and feeds into capacity planning and incident playbooks.

Overall NCSR Maturity Self-Rating: 4 - Managed

Governance (ID.GV)

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Sub-category	Mathspace alignment
RS.CO-1 Personnel know their roles and order of operations when a response is needed	The incident-response plan defines preparation, detection, containment, eradication, recovery and

Sub-category	Mathspace alignment
	post-incident steps. Roles and on-call rotations are documented; SquadCast alerts the 24x7 team and the first responder escalates per a severity matrix within five minutes.
RS.CO-2 Incidents are reported consistent with established criteria	Severity thresholds trigger mandatory notifications: affected customers within 24 h, regulatory bodies as required, and contracted districts within 72 h. All events are logged and reviewed after action.
RS.CO-3 Information is shared consistent with response plans	A public status page provides hourly updates until resolution; customer-specific impact summaries are emailed. Internal Slack channels and executive briefings run in parallel, ensuring consistent messaging.
RS.CO-4 Coordination with stakeholders occurs consistent with response plans	Comms leads coordinate with engineering, support, legal and executive teams, and reach out to law-enforcement or CERTs where necessary. Recovery milestones are reported to internal leadership and to customer contacts.
RS.CO-5 Voluntary information sharing occurs with external stakeholders to achieve broader situational awareness	Mathspace publishes post-incident reports on the status page, maintains a security@ mailbox for researchers, participates in industry groups and subscribes to threat-intelligence feeds to both share and consume insights.

Overall NCSR Maturity Self-Rating: 5 - Measured

Risk Assessment (ID.RA)

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Sub-category	Mathspace alignment
ID.RA-1 Asset vulnerabilities are identified and documented	A complete inventory of production assets is maintained and updated continuously. Authenticated host-level vulnerability scans run at least monthly, and all findings are entered into the central risk register with owners and due dates.
ID.RA-2 Threat intelligence is received and analysed	Mathspace ingests commercial and community threat-intelligence feeds and AWS GuardDuty findings. Indicators are reviewed daily; relevant items

Sub-category	Mathspace alignment
	update our likelihood scores and feed into hunting playbooks.
ID.RA-3 Threats are identified and documented	External penetration tests, continuous vulnerability discovery, and threat intelligence produce a living threat catalogue. The Security and Engineering leads review and refresh this catalogue every quarter.
ID.RA-4 Potential business impacts and likelihoods are identified	The annual enterprise risk assessment maps each threat to impact tiers that combine data sensitivity, service availability and regulatory exposure. Likelihood is calculated from historic incident metrics and industry data; results drive SLA targets (RTO 24 h / RPO 24 h).
ID.RA-5 Risk responses are identified and prioritised	Risks exceeding the "medium" threshold trigger a documented treatment plan: critical CVEs are patched within 24 h; residual risk may be transferred via cyber-liability insurance or formally accepted with CTO sign-off. Progress is tracked in the risk register.
ID.RA-6 Risk is managed to organisationally defined criteria	A risk matrix aligned to NIST CSF sets accept, mitigate, transfer or avoid criteria. Status is reported to senior management each quarter and used to drive budget and roadmap decisions.

Overall NCSR Maturity Self-Rating: 5 - Measured

Risk Management Strategy (ID.RM)

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Sub-category	Mathspace alignment
ID.RM-1 Risk management processes are established, managed, and agreed to by stakeholders	Mathspace operates a documented Information Security and Privacy Risk Management Framework. Asset classification (Confidential - Internal - Public) drives a central risk register maintained in Jira. Annual internal audits and quarterly management reviews verify that risks are identified, assessed, and treated. Supplier risks are assessed during onboarding and re-evaluated through contract renewals.

Sub-category	Mathspace alignment
ID.RM-2 Organizational risk tolerance is determined and clearly expressed	Executive leadership defines quantitative thresholds: uptime SLA 99.5 percent, RTO 24 h, RPO 24 h, and remediation windows of 24 h for critical and 72 h for high-severity vulnerabilities. Risks exceeding these limits require CTO approval and documented action plans.
ID.RM-3 Risk tolerance is informed by sector-specific analysis	Serving K-12 districts, Mathspace maps privacy obligations under FERPA and GDPR to its risk criteria and consults education security forums and ISACs for emerging threats. External assessments by education authorities validate that residual risk remains Low and inform updates to controls.

Overall NCSR Maturity Self-Rating: 4 - Managed

Supply Chain Risk Management (ID.SC)

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

Sub-category	Mathspace alignment
ID.SC-1 Cyber supply-chain risk management processes are established and agreed to	The Security Team maintains a documented Vendor Risk Management Policy that defines pre-contract due-diligence, onboarding checklists, risk tiers and review cadence. A vendor register in our GRC tool tracks ownership, status and next review dates; results are reported quarterly to the executive security forum.
ID.SC-2 Suppliers and partners are identified, prioritized and assessed	All third parties that handle production data or critical services are recorded in the vendor register and given a risk score based on data sensitivity, business impact and geographic location. High-risk providers (for example AWS and Cloudflare) undergo full questionnaires, SOC report reviews and background checks before approval.
ID.SC-3 Appropriate contractual requirements are in place	Master Service Agreements and DPAs require suppliers to implement MFA, encryption, incident reporting within 72 h, sub-processor flow-down, and right-to-audit clauses. Security schedules align with NIST CSF controls and require immediate notice of material changes.

Sub-category	Mathspace alignment
ID.SC-4 Suppliers are routinely evaluated for adherence to requirements	Critical suppliers are re-assessed annually through renewed security questionnaires, SOC 2 / ISO 27001 report reviews or penetration-test summaries. Findings are logged in the vendor register and tracked to closure; non-compliance triggers executive escalation or off-boarding.
ID.SC-5 Response and recovery planning is coordinated with suppliers	Incident Response and Business Continuity plans include supplier contact trees and joint test scenarios. Table-top exercises with hosting and CDN providers are run at least once per year; lessons learned feed back into both parties' playbooks and SLAs.

Overall NCSR Maturity Self-Rating: 4 - Managed

Identity Management, Authentication and Access Control (PR.AC)

Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Sub-category	Mathspace alignment
PR.AC-1 Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	Google Workspace is our source of truth for staff identities; student and teacher accounts flow in via SAML/Clever/ClassLink. Automated role-based provisioning assigns least-privilege access across AWS IAM, Git repos and SaaS tools. MFA is enforced for all staff logins. Off-boarding triggers immediate credential revocation, and quarterly audits verify account status and admin actions.
PR.AC-2 Physical access to assets is managed and protected	We host production workloads in AWS ISO 27001 facilities with 24x7 guards, CCTV and biometric entry. Corporate offices use electronic badge access, CCTV and alarm systems; a clear-desk policy and visitor logs reinforce protection of devices and paper records.
PR.AC-3 Remote access is managed	No always-on VPN is required; staff reach cloud services over TLS with MFA-protected SSO. Administrative shell access terminates at a hardened bastion that accepts key-based SSH only, with sudo escalation and full session logging.

Sub-category	Mathspace alignment
PR.AC-4 Access permissions and authorizations are managed, incorporating least privilege and segregation of duties	Role-based access control governs application, database and infrastructure layers. Change, code-review and release duties are separated; engineers cannot approve their own changes. Access reviews run quarterly and on personnel change, and all privileged actions are logged to a central SIEM.
PR.AC-5 Network integrity is protected (e.g., network segregation, segmentation)	Production, staging and development run in separate AWS accounts. Edge traffic is filtered by Cloudflare WAF before entering a DMZ; internal tiers are segmented with security groups and NACLs. Firewalls, IDS/IPS alerts and continuous log monitoring guard against lateral movement.
PR.AC-6 Identities are proofed, bound to credentials and asserted in interoperable ways	Users authenticate through district-issued SAML or OAuth2 providers, ensuring identity proofing occurs upstream. Unique user IDs follow through to our RBAC model, and session cookies are signed, HTTP-only and SameSite-strict to bind identity to every request.

Overall NCSR Maturity Self-Rating: 5 - Measured

Awareness and Training (PR.AT)

The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

Sub-category	Mathspace alignment
PR.AT-1 All users receive awareness training	Mandatory security and privacy training is completed by every employee at onboarding and at least once per year. Content covers policies, data protection, phishing, social-engineering awareness and is refreshed annually to reflect new threats.
PR.AT-2 Privileged users understand their roles	System administrators and developers undertake additional secure-coding and privileged-access training, reinforced by peer review and change-management checkpoints.
PR.AT-3 Third-party stakeholders understand their roles	Contractors, temps and other third parties sign confidentiality agreements and must finish Mathspace's security awareness module before any

Sub-category	Mathspace alignment
	access is granted, in line with contract clauses that mandate protective controls.
PR.AT-4 Senior executives understand their roles	Executives complete the same annual training as staff and review program performance in quarterly security governance meetings, ensuring accountability for risk management and resourcing.
PR.AT-5 Physical & cybersecurity personnel understand their roles	Dedicated security and IT personnel follow documented IR and physical-security procedures and participate in multi-annual tabletop and live incident exercises.

Overall NCSR Maturity Self-Rating: 4 - Managed

Data Security (PR.DS)

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Sub-category	Mathspace alignment
PR.DS-1 Data at rest is protected	All customer and internal data is encrypted at rest with AES-256 using AWS KMS-managed keys for RDS, S3 and EBS. Snapshots and backups inherit the same encryption and remain encrypted for their full retention period.
PR.DS-2 Data in transit is protected	TLS 1.2+ is enforced for every external and internal connection, including APIs and service-to-service traffic. HSTS is enabled and weak ciphers are disabled.
PR.DS-3 Assets are formally managed through removal, transfer and disposition	A central asset inventory is kept. Off-boarding requires return of equipment and immediate credential revocation. Retired media is cryptographically wiped or physically destroyed and certificates of destruction are retained.
PR.DS-4 Adequate capacity is maintained to ensure availability	Workloads run on autoscaling AWS services. Multi-AZ databases and redundant microservices support a 99.5 % SLA with 24 h RTO/RPO. Capacity and performance metrics are reviewed weekly.
PR.DS-5 Protections against data leaks are implemented	DLP controls cover outbound email and portable media. Cloudflare WAF, GuardDuty and

Sub-category	Mathspace alignment
	least-privilege IAM block unauthorised export. No student data is shared with advertising or analytics platforms.
PR.DS-6 Integrity-checking mechanisms are used	CI/CD pipeline runs software composition analysis plus static and dynamic security testing. Monthly authenticated vulnerability scans and AWS Inspector verify package integrity and alert on drift.
PR.DS-7 Development and testing environments are separate from production	Development, staging and production reside in isolated AWS accounts with no shared infrastructure. Only sanitised data is allowed in non-production environments and access keys are environment-scoped.

Overall NCSR Maturity Self-Rating: 4 - Managed

Information Protection Processes and Procedures (PR.IP)

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Sub-category	Mathspace alignment
PR.IP-1 Baseline configuration is created and maintained	Hardened "gold images" for AWS Linux and ScaleFusion-managed endpoints apply CIS benchmarks and least-functionality settings. Changes are tracked via IaC and reviewed quarterly.
PR.IP-2 System Development Life Cycle is implemented	Secure SDLC embeds threat modelling, secure design review, code review, SAST/DAST and annual third-party pentest inside the daily CI/CD pipeline.
PR.IP-3 Configuration change control processes are in place	A documented Change Management policy classifies changes, requires security sign-off through the CAB, stores artifacts, and enforces peer review before automated deployment.
PR.IP-4 Backups are conducted, maintained and tested	Encrypted point-in-time and daily backups replicate to a second region; automatic restore tests run daily and full DR drills run annually.
PR.IP-5 Physical operating-environment requirements are met	Production runs in AWS ISO 27001 data centers; offices use badges, CCTV and alarms. Environmental

Sub-category	Mathspace alignment
	and physical risks are reviewed with providers and logged in the risk register.
PR.IP-6 Data is destroyed according to policy	User data is obfuscated 90 days after deactivation and wiped from immutable backups after three months; retired media undergoes cryptographic wipe with certificates of destruction.
PR.IP-7 Protection processes are continuously improved	Post-incident reviews, monthly vulnerability trending and quarterly exec reviews feed corrective actions and policy updates.
PR.IP-8 Effectiveness of protection technologies is shared	GuardDuty, Security Hub and SIEM dashboards surface metrics that are discussed in weekly security stand-ups and reported to leadership each quarter.
PR.IP-9 Response and recovery plans are in place and managed	Documented IR, BC and DR plans define roles, triggers and communications; a 24 × 7 on-call team is paged via SquadCast.
PR.IP-10 Response and recovery plans are tested	IR tabletops and live drills occur several times per year; BC/DR failover is tested annually, and daily automated restores validate backup integrity.
PR.IP-11 Cybersecurity is included in HR practices	Role-based provisioning, annual access reviews, confidentiality agreements, security training on hire and yearly, and immediate de-provisioning on exit enforce least privilege.
PR.IP-12 Vulnerability management plan exists and is executed	Threat-intel feeds, daily scans, monthly authenticated scans, annual pentest and SLA-bound patch windows (24-72 h) are governed by a formal VM program.

Overall NCSR Maturity Self-Rating: 4 - Managed

Maintenance (PR.MA)

Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

Sub-category	Mathspace alignment
PR.MA-1 Maintenance and repair of organizational assets are performed and logged	A documented change-management process governs all configuration and software updates. Critical and high-severity patches are deployed inside 24 hours; routine updates are applied on a weekly cadence.

Sub-category	Mathspace alignment
	Maintenance activities are executed via automated tooling, recorded in AWS CloudTrail, and retained for at least six months. Administrative actions are formally reviewed to ensure completeness and policy compliance.
PR.MA-2 Remote maintenance is approved, controlled and logged	Remote access is limited to time-bound engineer sessions over SSH through a hardened bastion host, using individual key pairs and Google Workspace MFA. Each session requires an approved ticket under the change-management workflow, is fully logged in CloudTrail, and is monitored by GuardDuty.

Overall NCSR Maturity Self-Rating: 4 - Managed

Protective Technology (PR.PT)

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Sub-category	Mathspace alignment
PR.PT-1 Audit and log records are defined, implemented and reviewed	All production systems, networks and applications stream logs to centralized AWS CloudWatch and a SIEM. Logs cover authentication, data access and admin actions, are time-synchronized via three NTP sources, retained for at least six months and protected from alteration. On-call engineers triage SIEM alerts 24×7 and conduct monthly log reviews.
PR.PT-2 Removable media is protected and usage restricted	Removable media is not used in regular operations; backups replicate directly between encrypted AWS storage in multiple regions. Policy permits removable drives only for incident forensics, where full-disk encryption and chain-of-custody controls apply.
PR.PT-3 Least-functionality controls are enforced	Role-based access control ties every user to predefined roles with least-privilege permissions. Change management and automated configuration hardening ensure only required ports, protocols and services run in each environment. Access rights are reviewed quarterly and revoked immediately on off-boarding.
PR.PT-4 Communications and control networks are protected	Layered controls include Cloudflare WAF, AWS security groups, IDS/IPS, segregated VPC zones and

Sub-category	Mathspace alignment
	DMZs for internet-facing assets. All internal and external traffic carrying sensitive data is encrypted with TLS 1.2 or higher, and HSTS is enabled site-wide. Continuous monitoring raises real-time alerts on anomalous traffic.
PR.PT-5 Resilience mechanisms meet availability targets	Web and worker tiers run in auto-scaling groups behind redundant load balancers. Databases are multi-AZ with point-in-time recovery; daily snapshots replicate to a second region. Traffic can be rerouted between U.S. and Australian data centers within minutes, supporting an SLA of 99.5 percent, RTO 24 h and RPO 24 h.

Overall NCSR Maturity Self-Rating: 4 - Managed

Anomalies and Events (DE.AE)

Anomalous activity is detected and the potential impact of events is understood.

Sub-category	Mathspace alignment
DE.AE-1 Baseline of network operations is established and managed	VPC Flow Logs, application metrics and service health data are ingested into AWS CloudWatch and our SIEM to define "known-good" patterns for traffic volume, authentication success rates and API usage. Automated rules highlight deviations from this baseline, which are reviewed in a weekly log-hygiene session.
DE.AE-2 Detected events are analysed to understand attack targets and methods	Alerts from GuardDuty, Cloudflare WAF and IDS/IPS include contextual metadata (source, tactic, asset) and open an investigation ticket. Security engineers apply ATT&CK mapping and threat-intel enrichment to determine likely objectives and affected assets before assigning severity.
DE.AE-3 Event data are collected and correlated from multiple sources and sensors	Centralised logging (CloudWatch Logs, CloudTrail, VPC Flow Logs, OSSEC agents) streams into a managed SIEM where correlation rules stitch events across layers. Cross-source correlation cuts noise and enables single-pane triage of authentication anomalies, WAF blocks and host findings.
DE.AE-4 Impact of events is determined	The incident response plan defines four impact tiers combining data sensitivity, user scope and service

Sub-category	Mathspace alignment
	availability. During triage, responders run a scoped query across logs and asset inventory to measure blast radius, then document the impact tier in the incident record and status page update.
DE.AE-5 Incident alert thresholds are established	Alert thresholds are tuned for high-confidence indicators: critical GuardDuty findings, WAF anomaly scores, ≥ 5 failed logins in 60 s, CPU or error spikes above $3\times$ baseline. Squadcast routes pages to a 24×7 on-call engineer; median acknowledgement time is under five minutes, reviewed monthly.

Overall NCSR Maturity Self-Rating: 5 - Measured

Security Continuous Monitoring (DE.CM)

The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

Sub-category	Mathspace alignment
DE.CM-1 The network is monitored to detect potential cybersecurity events	Layered detection (Cloudflare WAF, AWS GuardDuty, signature / anomaly-based IDS / IPS) feeds centralized logging in CloudWatch and a SIEM. Alerts generate PagerDuty-style notifications to a 24×7 on-call rotation; events are triaged within five minutes and escalated per severity matrix.
DE.CM-2 The physical environment is monitored to detect potential cybersecurity events	AWS data centers provide 24×7 guard presence, CCTV and biometric access controls; Mathspace offices use electronic card access, alarms and CCTV. Facility risks are reassessed annually and any findings tracked to closure.
DE.CM-3 Personnel activity is monitored to detect potential cybersecurity events	All user and administrator actions (logon/logoff, privilege use, data changes) are written to immutable centralized logs. Role-based access reviews occur at least quarterly; anomalous behaviour triggers SIEM rules and human review.
DE.CM-4 Malicious code is detected	Centrally managed EDR and anti-malware scanners run on all servers and workstations; AWS Inspector performs daily vulnerability and malware scans. WAF signatures block known exploit payloads before they reach the application tier.

Sub-category	Mathspace alignment
DE.CM-5 Unauthorized mobile code is detected	Execution of unsigned or unmanaged binaries is prevented through EDR policy; web-delivered mobile code (e.g. JavaScript) is validated by the WAF and Content-Security-Policy headers. BYOD devices are brought under MDM before they can access corporate resources.
DE.CM-6 External service-provider activity is monitored to detect potential cybersecurity events	AWS CloudTrail records all API activity; GuardDuty analyses this stream for anomalous patterns. Vendor SOC reports and penetration-test deliverables are reviewed yearly, and contracts require timely security incident reporting.
DE.CM-7 Monitoring for unauthorized personnel, connections, devices and software is performed	Asset inventory is reconciled against DHCP / IAM logs; SIEM rules alert on unknown hosts, ports or software installs. MFA is enforced for all privileged accounts, and GuardDuty/IDS alert on suspicious network connections or brute-force attempts.

Overall NCSR Maturity Self-Rating: 5 - Measured

Detection Processes (DE.DP)

Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

Sub-category	Mathspace alignment
DE.DP-1 Roles and responsibilities for detection are defined	The Security Incident Response Plan assigns clear detection duties to the on-call engineering rotation, security lead and communications lead. Responsibilities cover log review, alert triage and stakeholder notification, ensuring accountability across all time zones.
DE.DP-2 Detection activities are tested	Detection tooling and runbooks are exercised at least annually and after major infrastructure changes. Table-top scenarios and live alert drills validate CloudWatch, GuardDuty, WAF and SIEM alerting as well as paging through SquadCast. Findings are tracked to closure.
DE.DP-3 Event detection information is communicated to appropriate parties	Alerts are triaged within five minutes and escalated by severity. Customers see real-time updates on status.mathspace.co (hourly cadence) and receive

Sub-category	Mathspace alignment
	direct email notice within 24 hours; critical incidents trigger stakeholder calls as required.
DE.DP-4 Detection processes are continuously improved	Every incident includes a post-mortem that captures root cause and missed signals. Lessons learned feed back into log-parsing rules, WAF signatures and SIEM correlation queries; metrics on mean-time-to-detect are reviewed monthly.
DE.DP-5 Detection processes comply with applicable requirements	Logging, monitoring and retention align with NIST CSF 1.1/2.0. Centralised SIEM collects alerts from IDS/IPS, WAF, EDR and cloud services, with six-month log retention and time-sync enforcement. Breach notification laws and district contracts require notification within 72 hours or sooner.

Overall NCSR Maturity Self-Rating: 5 - Measured

Response Planning (RS.RP)

Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

Sub-category	Mathspace alignment
RS.RP-1 Response plan is executed during or after an incident	Mathspace maintains a formally documented Incident Response Plan covering preparation, detection, containment, eradication, recovery and post-incident review. The plan is reviewed at least annually and exercised multiple times each year through tabletop and live drills. A 24 × 7 SquadCast on-call rotation is paged within five minutes of high-severity alerts; responders follow role-based runbooks and record actions in SquadCast. Customer and regulatory notifications are issued within required timeframes (≤ 72 h), and a public status page is updated hourly during major events. Post-mortems capture lessons learned to strengthen controls and update procedures.

Overall NCSR Maturity Self-Rating: 4 - Managed

Communications (RS.CO)

Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

Sub-category	Mathspace alignment
RS.CO-1 Personnel know their roles and order-of-operations	A formally approved incident response plan assigns clear responsibilities to Engineering, Security, Support and Executive stakeholders. A 24 × 7 on-call rotation is triggered by SquadCast within five minutes and follows runbooks that prioritise containment, eradication and customer communications.
RS.CO-2 Incidents are reported consistent with established criteria	Events are triaged against a severity matrix; security incidents are escalated to the Incident Commander and Executive team immediately, with customer and regulatory notification no later than 72 hours (or sooner if contractually required). Internal reporting flows through dedicated Slack channels and weekly post-incident reviews.
RS.CO-3 Information is shared consistent with response plans	The plan includes templated updates for internal leadership, affected customers and the public status page. Updates are posted hourly until resolution; affected customers receive direct email within 24 hours and final root-cause analysis on closure.
RS.CO-4 Coordination with stakeholders occurs consistent with response plans	The cross-functional response team coordinates with Legal, Public Relations and Customer Success to ensure unified messaging. External forensic support can be engaged, and liaison procedures for law-enforcement contact are documented and rehearsed.
RS.CO-5 Voluntary information sharing with external parties	The Security team maintains trusted relationships with AWS, Cloudflare, industry ISACs and law-enforcement agencies. Indicators of compromise and lessons learned are shared responsibly to improve sector-wide resilience.

Overall NCSR Maturity Self-Rating: 5 - Measured

Analysis (RS.AN)

Analysis is conducted to ensure effective response and support recovery activities.

Sub-category	Mathspace alignment
RS.AN-1 Notifications from detection tools are investigated	Centralised logging (AWS CloudWatch, SIEM) aggregates Cloudflare WAF, GuardDuty, IDS/IPS and vulnerability scan alerts. The 24 × 7 on-call rotation is

Sub-category	Mathspace alignment
	paged via SquadCast; engineers triage within five minutes and start incident tickets that link logs and timelines.
RS.AN-2 Incident impact is understood	The Incident Response Plan defines severity tiers that blend data sensitivity, user scope and service availability. Impact analysis is led by the incident commander and updated continuously; customer status updates are posted hourly and directly emailed inside 24 hours.
RS.AN-3 Forensics are performed	Chain-of-custody and evidence-preservation procedures guide log capture, disk images and memory dumps. Dedicated forensics workstations and encrypted evidence vaults support root-cause analysis and any regulatory or legal needs.
RS.AN-4 Incidents are categorised consistent with response plans	Events are mapped to predefined categories (e.g. unauthorised access, data disclosure, service degradation) that drive escalation paths, communications templates and regulatory notice requirements. Metrics from each category feed post-incident reviews.
RS.AN-5 External vulnerability and threat data are analysed	A formal Threat & Vulnerability Management programme consumes threat-intelligence feeds and researcher disclosures (security@mathspace.co). Issues are risk-ranked, reproduced, and either patched or mitigated within SLA (24 h for critical, 72 h for high).

Overall NCSR Maturity Self-Rating: 4 - Managed

Mitigation (RS.MI)

Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

Sub-category	Mathspace alignment
RS.MI-1 Incidents are contained	SquadCast alerts our 24 × 7 on-call engineers within five minutes of detection. Standard runbooks mandate rapid containment: isolate impacted AWS security groups, revoke exposed credentials, and block malicious traffic at the Cloudflare WAF while preserving forensic evidence.

Sub-category	Mathspace alignment
RS.MI-2 Incidents are mitigated	The incident response plan directs eradication, recovery and communication. Encrypted point-in-time backups enable data restoration; emergency change management deploys fixes; the public status page is updated hourly until normal service and monitoring confirm stability.
RS.MI-3 Newly identified vulnerabilities are mitigated or risk-accepted	Daily automated scans, monthly external scans and threat-intel feeds create Jira tickets with SLAs: critical fixes within 24 h, high within 72 h. Deferred items require documented risk acceptance by the CTO and tracking in the quarterly security review.

Overall NCSR Maturity Self-Rating: 4 - Managed

Improvements (RS.IM)

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Sub-category	Mathspace alignment
RS.IM-1 Response plans incorporate lessons learned	After every incident we run a structured post-mortem that documents root cause, timeline, impact and corrective actions. Findings are reviewed by the security lead and fed into playbooks, the Data Breach Response Plan and on-call runbooks. Lessons learned are shared in engineering all-hands and tracked through Jira until verified in the next response drill.
RS.IM-2 Response strategies are updated	The incident response plan is exercised multiple times per year, including joint supplier scenarios. Metrics such as mean time to detect, contain and remediate are trended; when targets slip, the response strategy is revised, tooling is tuned (e.g. GuardDuty rules, SIEM alerts) and staff retrained. Updates are version-controlled and re-approved by senior management.

Overall NCSR Maturity Self-Rating: 5 - Measured

Recovery Planning (RC.RP)

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

Sub-category	Mathspace alignment
RC.RP-1 Recovery plan is executed during or after a cybersecurity incident	Mathspace maintains a documented Disaster Recovery and Business Continuity Plan covering people, processes, technology and alternate sites. Critical workloads operate across two AWS regions with near real time replication and automated daily backups. The plan sets an RTO of 24 h and an RPO of 24 h, and on-call leads trigger runbooks within five minutes of a major incident. Full restoration drills occur at least annually (last exercised December 2024), with weekly environment rebuild tests and daily point-in-time database restores to verify backup integrity.

Overall NCSR Maturity Self-Rating: 4 - Managed

Improvements (RC.IM)

Recovery planning and processes are improved by incorporating lessons learned into future activities.

Sub-category	Mathspace alignment
RC.IM-1 Lessons learned are incorporated	Every incident or recovery exercise closes with a structured after-action review led by the Security Team. Root-cause analyses and corrective actions are logged, prioritised, and tracked through our change-management workflow, guaranteeing that playbooks, runbooks, and automation scripts are updated before the next sprint.
RC.IM-2 Recovery strategies are updated	Outputs from post-mortems and the annual disaster-recovery test drive revisions to the Business Continuity Plan and service-level objectives. The CTO signs off updated RTO/RPO targets and engineering tickets ensure new controls are rolled out company-wide and verified in the next quarterly drill.

Overall NCSR Maturity Self-Rating: 4 - Managed

Communications (RC.CO)

Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

Sub-category	Mathspace alignment
RC.CO-1 Public relations are managed	The incident response plan assigns a dedicated communications lead and provides media templates. During an event we publish updates on status.mathspace.co and, if appropriate, coordinate statements with district communications staff.
RC.CO-2 Reputation is repaired after an incident	Post-incident reviews include executive sign-off on customer-facing remediation actions such as credit offers or service-fee credits. Findings feed into a continuous improvement backlog and are summarised on the public status page to maintain transparency and trust.
RC.CO-3 Recovery activities are communicated to internal stakeholders and executive and management teams	Outages trigger PagerDuty alerts to a 24 × 7 on-call engineering rota and automatic notifications to an internal Slack war-room. Incident commanders issue hourly progress briefs and a final RCA to senior leadership.
RC.CO-4 Recovery activities are communicated to external stakeholders as appropriate	Affected customers receive email notification within 24 hours, and major districts are contacted directly per contract (≤ 72 hours). The status page is updated at least hourly until resolution, and support channels provide real-time guidance on workarounds.

Overall NCSR Maturity Self-Rating: 4 - Managed







MathSpace_FrederickCounty_VA_14State_OHG

Final Audit Report

2025-10-27

Created:	2025-10-27
By:	TEC SDPA (bbirdsall@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAs1Lt6Ny30psmYBY21LjU5jEODrv3Xc9h

"MathSpace_FrederickCounty_VA_14State_OHG" History

-  Document created by TEC SDPA (bbirdsall@tec-coop.org)
2025-10-27 - 2:35:27 PM GMT
-  Document emailed to Rhonda Davis (rdavis@mathspace.com.au) for signature
2025-10-27 - 2:35:56 PM GMT
-  Email viewed by Rhonda Davis (rdavis@mathspace.com.au)
2025-10-27 - 3:11:05 PM GMT
-  Signer Rhonda Davis (rdavis@mathspace.com.au) entered name at signing as Mohamad Jebara
2025-10-27 - 3:12:38 PM GMT
-  Document e-signed by Mohamad Jebara (rdavis@mathspace.com.au)
Signature Date: 2025-10-27 - 3:12:40 PM GMT - Time Source: server
-  Agreement completed.
2025-10-27 - 3:12:40 PM GMT






Mathspace_FrederickCounty_VA_14state_OHG_vendorsigned

Final Audit Report

2025-10-27

Created:	2025-10-27
By:	TEC SDPA (bbirdsall@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAW81z0lb8F8nmqy5tghCP6vDFGbqxnyj

"Mathspace_FrederickCounty_VA_14state_OHG_vendorsigned" History

-  Document created by TEC SDPA (bbirdsall@tec-coop.org)
2025-10-27 - 3:19:28 PM GMT
-  Document emailed to Timothy Grant (grantt@fcpsk12.net) for signature
2025-10-27 - 3:19:43 PM GMT
-  Email viewed by Timothy Grant (grantt@fcpsk12.net)
2025-10-27 - 6:45:04 PM GMT
-  Document e-signed by Timothy Grant (grantt@fcpsk12.net)
Signature Date: 2025-10-27 - 6:45:50 PM GMT - Time Source: server
-  Agreement completed.
2025-10-27 - 6:45:50 PM GMT