

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

Regional School Unit #14 Windham Raymond Schools

and

Ayasis Yazılım ve Bilişim Teknolojileri Anonim Şirketi

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: Regional School Unit #14 Windham Raymond Schools, located at 228 Windham Center Rd., Windham, ME 04062 USA (the “**Local Education Agency**” or “**LEA**”) and Ayasis Yazılım ve Bilişim Teknolojileri Anonim Şirketi, located at Unit 6 Queens Yard, White Post Lane, London UK E9 5EN (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: Basar Kaya Title: Head of Business Development

Address: Unit 6 Queens Yard, White Post Lane, London UK E9 5EN

Phone: +358452621990 Email: basar@mentalup.co

The designated representative for the LEA for this DPA is:

Bob Hickey, Technology Director
228 Windham Center Rd., Windham, ME 04062
207-892-1800 rhickey@rsu14.org

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

Regional School Unit #14, Windham Raymond Schools

By: Mike Duffy Date: 12/08/2025
Mike Duffy (Dec 8, 2025 13:53:51 EST)

Printed Name: Michael Duffy Title/Position: Risk and Safety Specialist

Ayasis Yazılım ve Bilişim Teknolojileri Anonim Şirketi

By:  Date: 23.07.2025

Printed Name: EMRE OZGUNDUZ Title/Position: Managing Director & Co-Founder

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

MentalUP: Gamified exercises to develop cognitive skills with performance reports showing strengths and areas for improvement.

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.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
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	X
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	X
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if Used by Your System
Schedule	Student scheduled courses	
	Teacher names	X
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	X
	State ID number	
	Provider/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

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:	<p>The user's device token ID is stored (with user consent) for the purpose of sending in-app notifications.</p> <p>Scores from educational games are stored to provide personalized content to the user.</p> <p>If the user participates in standard in-app tests or quiz activities, their scores are stored to track and report learning progress.</p>
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT “C”

DEFINITIONS

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

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

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

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an “operator” for the purposes of this section.

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

Provider: For purposes of the DPA, the term “Provider” means 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 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 checked="" 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”
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"

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"
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.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Communications	Online communications that are captured (emails, blog entries)	
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify:	
Personal Contact Information	Personal Address	
	Personal Email	x
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses	
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Teacher app username	x
	Teacher app passwords	x
Teacher In App Performance	Program/application performance	
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	
	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

<https://www.mentalup.co/agreements/data-security-and-privacy-plan>



Emre OZGUNDUZ
Managing Partner of MentalUP

Data Security and Privacy Plan

1. This Data Security and Privacy Plan (“**Plan**”) was executed by and between Ayasis Yazılım ve Bilişim Teknolojileri Anonim Şirketi (“**the Company**”) located at Yıldız Teknik Üniversitesi Davutpaşa Kampüsü Teknopark D2 Blok No: 1B06 Esenler/Istanbul in its capacity as the “**Data Controller**” and applies all individuals (“**Member**”) who use the MentalUP products/services through www.mentalup.net and www.mentalup.co web sites and MentalUP mobile application (“**MentalUP**”) owned and operated by the Company. In this context, the purpose of this Plan is to provide information on the collection, processing and use of the data provided by you in connection with the use of MentalUP as well as the grade, purpose and scope of transfer thereof.
2. When a Member uses MentalUP or communicates with MentalUP in any way, MentalUP collects information about the Member, in accordance with the nature of the information and transaction, within the limits of existing technical capabilities. The Member acknowledges, declares, and undertakes that their personal information and data may be used by the Company and/or through MentalUP in the manner and for the purposes specified in this Plan.
3. The Company might collect the Member's personal information (user name, name if provided, IP address, the date and time of access, the pages accessed while being on MentalUP) and the activities taken place under MentalUP in order to provide better service to the Member, to make suggestions, to improve its services, to facilitate the use of MentalUP at the works related to the Member's interests and preferences, within the framework of legal legislation.
4. The information provided by the Member in order for the Company to communicate with itself as well as the information obtained by the Company via cookies and similar technologies during the Member’s activities on MentalUP; might be recorded, stored in printed / magnetic archives, updated whenever necessary, shared, transferred, used and processed by the Company in accordance with the personal data processing requirements and purposes set out in the applicable legislation. The information obtained may also be shared, transferred or processed by the Company’s current and future affiliates, subsidiaries, shareholders, business partners, domestic and/or international program partners, service providers or third parties (including but not limited to legal and tax consultants, banks, and independent auditors) in order to carry out the Company's services and operations, to provide the services offered, and to fulfill related legal or contractual obligations. This also includes providing certain services to you in connection with the use of MentalUP, to fulfill the necessary procedures for payment in the event that the goods and services provided are subject to any fee, to inform regarding the services rendered, to be able to respond to questions, to make sure that the necessary permits are received and taken from parents/legal representatives if the Member is between the ages of 13 and 18, if it is required directly for the execution and performance of a contract between the Company and the Member and for the Company to fulfill its legal obligations and also for the purposes of asserting the relevant rights or establishing the defense in relation to such personal data, limited to the purpose of use, and for a period of time limited with such use.. This information shared may be changed and updated by the Member at any time. Data collected through MentalUP may not be used or shared with third parties for purposes unrelated to improving the user experience or software/hardware performance connected to the MentalUP’s functionality.

5. The data shared by the Member shall not be used directly or indirectly for the benefit of any third party for any reason whatsoever; without the express and explicit written permission of the Member, shall not be shared, partly or completely copied and published with any third party, firm or entity other than for the purposes set forth in this Plan. Additional authorization from the Member may be required if it is compulsory within the provisions of the relevant legislation or if the data transmitted by the Member must be used for purposes other than those specified in this text. In this case, the Member will be contacted, and its explicit consent will be requested. If the Member does not agree, no additional data shall be obtained.
6. If the personal data provided to the Company by the Member is requested by official institutions/organizations as necessitated by the law, the data may be transmitted to the relevant authorities and courts if requested by the courts.
7. It may be required to open an account in order to have access to the services of the Company. The Member declares that he or she is at least 18 years old (or older) and they understand and accept these conditions in order to open an account on his behalf. If the Member is under the age of 18 but at least 13 years old and has the authority to exercise discretion, they may only provide their data in the presence of one of their parents or a legal representative. In this context, the Member declares that his or her parent or legal representative has reviewed and accepted this Plan and that the data has been shared following the said permission. Neither person under 13 (thirteen) years of age can be directly a Member of the MentalUP itself, nor submit his/her own personal data directly.
8. In the event that the internet sites of the Company contain links to other internet sites according to the nature of the situation, the Company shall have no commitment to ensure that the operators of these sites comply with the data protection provisions. The Company shall never be responsible for the content of the sites to which it links with other methods such as links or the like.
9. Within the scope of the data you have provided to the Company, the Member may apply to the Company and be entitled to;
 - find out whether personal data is being processed;
 - request information on personal data, if it has been processed;
 - find out the purpose of processing his/her personal data and whether they are being used appropriately in line with their purposes;
 - know the third parties to whom personal data is transmitted in or out of the country;
 - request that his/her personal data be corrected if it is incomplete or incorrectly processed;
 - request that personal data be erased or destroyed if the circumstances requiring the processing of the personal data disappearance;
 - require correction, deletion or destruction to be reported to a third party to whom personal data is transferred;
 - object to the occurrence of an adverse consequence by analyzing the processed data exclusively through automated systems; and
 - have the right to claim damages in case of impairment because his/her personal data is processed in violation of the relevant legal legislation.

10. In the event that a Member submits his/her claims for his/ her rights towards the Company in the manner set forth in this Plan, the Company shall conclude the application as soon as possible and in any event not later than 30 (thirty) days in accordance with the nature of the claim.
11. Despite the fact that the processing activity is carried out in accordance with the relevant legislation, the personal data of the Member shall be deleted, destroyed or anonymized in accordance with the related legislation after the end of the processing purposes stated in this Plan.
12. In order to use the rights notified to the Member in this Plan, the Member must include the necessary information that can be used by the Company to identify the Member and the description/explanations regarding which right he/she requests to exercise must be delivered to Yıldız Technical University Davutpaşa Campus at Kampüsü Teknopark D2 Blok No:1B06 Esenler/Istanbul by hand or sent through notary or other methods specified in the related legislation or may be sent as signed by secure electronic signature to info@ayasis.com, which is the e-mail address of the Company. The Company accepts the request on the application of the Member or rejects it by explaining the reason and declares the answer to the related person in writing or in electronic form. If the application is accepted, it will be fulfilled by the Company. If the applicant is attributable to any fault of the Company and a fee is collected from the Member, the remuneration shall be returned to the Member.
13. The Company undertakes to keep the Member's data and any confidential information strictly private and confidential, without prejudice to the contents hereof, to regard it as an obligation to keep confidentiality, to take all measures and act in due diligence to prevent all or any part of the Member's information from entering into the public domain or be subject to unauthorized use, or to take measures to prevent the confidential information from disclosure to any third party. If, despite all necessary data security measures taken by the Company, the confidential information is damaged as a result of attacks on the system or captured by third parties, the Company shall have no responsibility with that respect.
14. The Company's data security measures are as follows:
 - Access logs are regularly maintained.
 - Corporate policies regarding access, information security, usage, storage, and disposal have been prepared and implemented.
 - Confidentiality agreements are in place.
 - Access rights related to data security are revoked for employees who change roles or leave the company.
 - Policies and procedures for the protection of personal data have been established.
 - The security of personal data is actively monitored.
 - Necessary security measures are in place for entry and exit to physical environments containing personal data.
 - Physical environments containing personal data are secured against external risks (e.g., fire, flood, etc.).
 - Security of environments containing personal data is ensured.

- Personal data is minimized as much as possible.
 - Personal data is backed up, and the security of these backups is ensured.
 - Internal periodic and/or random audits are conducted or commissioned.
 - Existing risks and threats have been identified.
 - Disciplinary regulations including data security provisions are in place for employees.
 - Regular training and awareness activities on data security are provided to employees.
 - Protocols and procedures for the protection of sensitive personal data have been established and are in practice.
 - Signed contracts include data security provisions.
 - Data encryption is applied.
15. The Company ensures the implementation of data security and privacy requirements throughout the contract in accordance with internal policies aligned with applicable data protection legislation. Access controls, secure data storage, and encryption protocols are consistently applied during the collection, processing, and transmission of data. Access to sensitive information is restricted to authorized personnel only.
 16. The Company implements administrative safeguards, including staff training, written security policies, and access control procedures. The Company applies operational safeguards such as role-based access, session logging, and regular reviews of user activity. The Company also enforces technical safeguards, including encryption (both in transit and at rest), firewalls, and secure authentication mechanisms such as two-factor authentication.
 17. The Company's employees and subcontractors with access to personally identifiable information receive training on the processing and protection of personal data, data privacy, secure communication practices, and incident response procedures
 18. All employees and subcontractors undergo annual training on data privacy and FERPA/Ed Law 2-d compliance. New team members complete onboarding training within their first week. Training covers the handling of personally identifiable information, secure communication practices, and incident response procedures.
 19. The Company requires all employees and subcontractors to sign confidentiality and data privacy agreements. These agreements include specific clauses about compliance with the contract and applicable state and federal data privacy laws.
 20. The Company maintains a documented Incident Response Plan. The Company reports any suspected or confirmed data breaches involving personally identifiable information to the The Educational Agency ("EA") within 24 hours. Root causes are investigated and corrective actions are implemented accordingly. Breach logs and reports are archived and provided upon request.
 21. The Company returns all relevant data to the EA using encrypted transmission methods upon completion of contractual obligations or when the data is no longer required. The transfer is executed over secure, access-controlled channels and is accompanied by a detailed data

transfer report. The EA is required to confirm receipt and integrity of the transferred data prior to data deletion from the Company's systems.

22. The Company securely destroys data using methods compliant with NIST SP 800-88. A certificate of destruction is generated and submitted to the EA upon completion. For cloud-based records, secure deletion is carried out through platform-specific data removal protocols.
23. The Company's data security and privacy program is reviewed and updated regularly to ensure alignment with EA policies. All custom configurations, data retention timelines, and user roles are adjusted to meet the specific privacy requirements provided by the EA.

24. The Company's Identity Regarding Data Security

- **Asset Management,** The Company regularly reviews and updates its data security and privacy program to ensure alignment with EA policies. Custom configurations, data retention periods, and user roles are tailored to EA's specific privacy requirements. The Company documents and tracks all data, devices, and systems involved in delivering its services. Access to data is role-based and limited to authorized personnel. The Company maintains an inventory of critical assets and regularly reviews access logs to ensure proper usage and compliance with internal policies.
- **Business Environment,** The Company's platform is designed to support personalized educational experiences for students. The Company prioritizes user privacy, regulatory compliance, and secure data practices in alignment with its mission. The Company reviews stakeholder needs (e.g., schools, students, parents) during feature planning and security assessments.
- **Governance,** The Company maintains internal policies for data security, access control, and incident response. The Company requires all team members to review and adhere to these policies. Governance practices are implemented in accordance with the legal rules applicable to our company regarding personal data.
- **Risk Assessment,** The Company conducts internal risk assessments regularly to identify potential threats to user data, including unauthorized access and service misuse. The Company utilizes technical audits and automated monitoring tools to detect and prioritize security risks that may impact organizational operations or users.
- **Risk Management Strategy,** The Company's risk strategy defines thresholds and response plans for security incidents. The Company categorizes risks by severity and documents action plans for high-risk items. The Company takes startup constraints into account when assigning risk tolerances and controls.
- **Supply Chain Risk Management,** The Company's platform relies on secure third-party cloud providers (e.g., AWS, Azure) and complies with their published data protection

standards (e.g., SOC 2, ISO 27001). The Company reviews vendor documentation annually and avoids using third-party tools that lack sufficient security transparency.

25. Data Security Protection Methods

- **Identity Management, Authentication and Access Control,** The Company restricts access to systems and databases to authorized personnel via role-based access controls. The Company enforces authentication using strong credentials, and limits administrative access to backend developers. The Company uses Azure Identity Management and AWS IAM tools where applicable.
- **Awareness and Training,** The Company briefs team members on cybersecurity best practices during onboarding, including the handling of sensitive educational data. Although formal training is not conducted regularly, The Company clearly defines and communicates responsibilities related to student data protection and Ed Law § 2-d internally.
- **Data Security,** The Company encrypts user data in transit and at rest using industry standards (e.g., TLS, AES-256). The Company restricts data access to essential personnel and maintains audit trails through platform-level monitoring. The Company follows a minimal data collection approach to reduce exposure.
- **Information Protection Processes and Procedures,** The Company maintains a publicly available Plan that outlines its data handling practices, including access controls, breach response, and secure data destruction. The Company follows internal procedures in accordance with this plan, which are reviewed regularly.
- **Maintenance,** The Company applies system updates and patches regularly using platform-level management tools (e.g., Azure automatic updates, AWS automatic updates). The Company operates exclusively cloud-based systems with no unmanaged physical components, thereby minimizing hardware-level maintenance risks.
- **Protective Technology,** The Company's cloud infrastructure includes protective technologies such as network-level firewalls, access controls, and encrypted storage. The Company utilizes both Microsoft Azure and Amazon Web Services (AWS) platforms. On Azure, The Company uses Azure Security Center to monitor configurations and receive recommendations for improving system security and resilience. On AWS, The Company employs services such as AWS Shield, AWS WAF, CloudTrail, and Security Hub to protect its infrastructure against unauthorized access, DDoS attacks, and misconfigurations. The Company encrypts data at rest using AWS KMS and in transit using TLS.

26. Detecting Data Breach Risks

- **Anomalies and Events,** The Company leverages logging and monitoring capabilities across both Azure and AWS to detect unusual activity, including repeated failed login attempts, abnormal data access patterns, and suspicious request behavior. The Company

uses tools such as Azure Monitor, CloudWatch, CloudTrail, and AWS GuardDuty to track system events, monitor user and API behavior, and identify potential threats in real time.

- **Security Continuous Monitoring,** The Company continuously monitors system activity using diagnostics, performance insights, and cloud-native alerting tools available in both Azure and AWS. The Company utilizes services such as Azure Monitor, Application Insights, Log Analytics, CloudWatch, AWS Config, and Security Hub to track system health, detect anomalies, and ensure security compliance. The Company periodically reviews logs and configures automated alerts for critical events, including unauthorized access attempts and configuration changes.
- **Detection Processes,** The Company implements detection processes using built-in monitoring and alerting tools provided by its cloud infrastructure. The Company enables logging at key points across the system and configures alerts for events such as failed logins and unexpected usage patterns. These processes are reviewed and tested during development and system updates to ensure timely awareness of potential security incidents.

27. Responding to Data Breaches

- **Response Planning,** The Company maintains an internal incident response plan that outlines the steps to be taken in the event of a security breach or system compromise. The Company assigns clear roles to team members and documents escalation paths to ensure a coordinated and timely response.
- **Communications,** The Company coordinates communication of response activities through designated internal team members, ensuring that responsibilities and actions are clearly distributed across relevant roles. When incidents affect educational data or require escalation, The Company informs the EA according to pre-established procedures. The Company maintains the ability to collaborate with external partners, such as legal advisors or cybersecurity consultants, as needed.
- **Analysis,** The Company reviews logs and system activity during and after an incident to understand the root cause and potential impact. The Company uses Azure and AWS monitoring tools to assist in forensic analysis and to ensure proper containment and follow-up actions.
- **Mitigation,** if a threat is detected, The Company immediately restricts access to affected systems and applies patches or configuration changes to prevent further spread. The Company isolates any compromised data or systems for analysis and remediation.
- **Improvements,** The Company reviews and documents lessons learned internally after each incident. Where applicable, The Company updates detection rules, access controls, and team procedures to reduce the likelihood of similar incidents in the future.

28. Data Recovery

- **Recovery Planning,** The Company maintains cloud-based backup and recovery processes to ensure minimal disruption in the event of a cybersecurity incident. The Company restores key assets and configurations using platform-native tools such as Azure Backup or AWS Backup, depending on the deployment.
- **Improvements,** The Company reviews recovery procedures after incidents to identify process gaps or delays. The Company adjusts recovery scripts, automation tools, and team roles as needed based on post-incident evaluations.
- **Communications,** in the recovery phase, The Company keeps relevant stakeholders—including the EA—informed of system restoration timelines and actions taken. The Company handles internal communications via assigned leads and notifies external parties when required.

41. The Company shall not disclose personal data and confidential information of the Member unless (a) it is required to disclose such information in accordance with applicable laws or regulations or a court decision or administrative order issued and/or (b) it is Member's request and/or (c) it is stated within this Plan or within other agreements executed by and between the Member and the Company.

42. The Company shall not be responsible for damages caused by the use of information that the member discloses in comments made or messages given by third parties in public areas. If the member shares his/her name, password, etc. used by the member when creating the membership record with third parties, the Company shall not be responsible for any damages that may arise from the information shared with third parties.

44. The Company may at any time update, amend, or revoke the provisions of this Plan. In this case, the Member shall be notified via the services/products or by other means such as e-mail. Any provision that is updated, modified or removed from effect shall enure for the Member at the time of publication. The Member shall be deemed to have accepted such amendment if the Member continues to use the services or products of the Company after such modification has been made.

Ayasis Yazılım ve Bilişim Teknolojileri Anonim Şirketi

DATA PRIVACY AND SECURITY PLAN

Provider DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party provider include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the provider **must complete the following or provide a plan that materially addresses its requirements**, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, providers should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	We implement data security and privacy requirements throughout the contract by following internal policies aligned with the applicable data protection legislation. Access controls, secure data storage, and encryption protocols are enforced consistently during data collection, processing, and transmission. Only authorized personnel are permitted to access sensitive information.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Administrative safeguards include staff training, written security policies, and access control procedures. Operational safeguards include role-based access, session logging, and regular review of user activity. Technical safeguards include encryption (in transit and at rest), firewalls, and secure authentication mechanisms (e.g., two-factor authentication).
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	The Company's employees and subcontractors with access to personally identifiable information receive training on the processing and protection of personal data, data privacy, secure communication practices, and incident response procedures.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	We require all employees and subcontractors to sign confidentiality and data privacy agreements. These agreements include specific clauses about compliance with the contract and applicable state and federal data privacy laws.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	We maintain a documented Incident Response Plan. Any suspected or confirmed data breaches involving personally identifiable information are reported to the EA within 24 hours. We also investigate root causes and apply corrective actions. Breach logs and reports are archived and shared upon request.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon completion of contractual obligations or when data is no longer required, all relevant data is returned to the EA using encrypted transmission methods. The transfer is executed over secure, access-controlled channels and is accompanied by a detailed data transfer report. The EA is required to confirm receipt and integrity of the transferred data prior to data deletion from our systems.

7	Describe your secure destruction practices and how certification will be provided to the EA.	Data is securely destroyed using NIST SP 800-88 compliant methods. A certificate of destruction is generated and submitted to the EA upon completion. For cloud-based records, secure deletion is conducted via platform-specific data removal protocols.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Our data security and privacy program is reviewed and updated regularly to ensure alignment with EA policies. All custom configurations, data retention timelines, and user roles are adjusted to meet the specific privacy requirements provided by the EA.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Provider's Data Privacy and Security Plan. Provider should complete the Provider Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. 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>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	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.	All data, devices, and systems involved in delivering our services are documented and tracked. Access is role-based and limited to authorized personnel. We maintain an inventory of critical assets and regularly review access logs to ensure proper usage and compliance with internal policies.
	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.	Our platform is designed to support personalized educational experiences for students. We prioritize user privacy, compliance with regulations, and secure data practices in alignment with our mission. Stakeholder needs (e.g., schools, students, parents) are reviewed during feature planning and security assessments.
	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.	We maintain internal policies for data security, access control, and incident response. All team members are required to review and adhere to these policies. Governance practices are implemented in accordance with the legal rules applicable to our company regarding personal data. .
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	We conduct internal risk assessments regularly to identify potential threats to user data, including unauthorized access and service misuse. Technical audits and automated monitoring tools help us detect and prioritize security risks that may impact organizational operations or users.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Our risk strategy defines the thresholds and response plans for security incidents. Risks are categorized by severity, and action plans are documented for high-risk items. Startup constraints are taken into account when assigning risk tolerances and controls
	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	Our platform relies on secure third-party cloud providers (e.g., AWS, Azure) and complies with their published data protection standards (e.g., SOC 2, ISO 27001). We review vendor documentation annually and avoid using third-party tools that lack sufficient security transparency.

Function	Category	Contractor Response
	processes to identify, assess and manage supply chain risks.	
PROTECT (PR)	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.	Access to systems and databases is restricted to authorized personnel via role-based access controls. Authentication is enforced using strong credentials, and administrative access is limited to backend developers. Azure Identity Management and AWS IAM tools are used where applicable.
	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.	Team members are briefed on cybersecurity best practices during onboarding, including the handling of sensitive educational data. Although formal training is not conducted regularly, responsibilities related to student data protection and Ed Law § 2-d are clearly defined and communicated internally.
	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.	User data is encrypted in transit and at rest using industry standards (e.g., TLS, AES-256). Data access is restricted to essential personnel and audit trails are maintained through platform-level monitoring. We follow a minimal data collection approach to reduce exposure.
	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.	We maintain a publicly available Privacy Policy that outlines our data handling practices, including access controls, breach response, and secure data destruction.. Internal procedures are followed in accordance with this policy and are reviewed regularly.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	System updates and patches are applied regularly using platform-level management tools (e.g., Azure automatic updates, AWS automatic updates). There are no unmanaged physical components; all systems are cloud-based, minimizing hardware-level maintenance risks.
	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.	Our cloud infrastructure includes protective technologies such as network-level firewalls, access controls, and encrypted storage. We utilize both Microsoft Azure and Amazon Web Services (AWS) platforms. On Azure, we use Azure Security Center to monitor configurations and receive recommendations for improving system security and resilience. On AWS, services such as AWS Shield, AWS WAF, CloudTrail, and Security Hub are used to protect our infrastructure against unauthorized access, DDoS attacks, and misconfigurations. Data is encrypted at rest using AWS KMS and in transit using TLS.
	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	The application leverages logging and monitoring capabilities across both Azure and AWS to detect unusual activity, including repeated failed login attempts, abnormal data access patterns, and suspicious request behavior. Tools such as Azure Monitor, CloudWatch, CloudTrail, and AWS GuardDuty are used to track system events, monitor user and API behavior, and identify potential threats in real time.

DETECT (DE)	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	System activity is continuously monitored using diagnostics, performance insights, and cloud-native alerting tools available in both Azure and AWS. We utilize services such as Azure Monitor, Application Insights, Log Analytics, CloudWatch, AWS Config, and Security Hub to track system health, detect anomalies, and ensure security compliance. Logs are periodically reviewed, and automated alerts are configured for critical events, including unauthorized access attempts and configuration changes.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Detection processes are implemented using built-in monitoring and alerting tools provided by our cloud infrastructure. Logging is enabled at key points across the system, and alerts are configured for events such as failed logins and unexpected usage patterns. These processes are reviewed and tested during development and system updates to ensure timely awareness of potential security incidents.
Function	Category	Contractor Response
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	We maintain an internal incident response plan that outlines the steps to be taken in the event of a security breach or system compromise. Team members are assigned clear roles, and escalation paths are documented to ensure a coordinated and timely response.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Communication of response activities is coordinated through designated internal team members, ensuring that responsibilities and actions are clearly distributed across relevant roles. When incidents affect educational data or require escalation, the EA is informed according to pre-established procedures. We maintain the ability to collaborate with external partners, such as legal advisors or cybersecurity consultants, as needed.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Logs and system activity are reviewed during and after an incident to understand the root cause and potential impact. Azure and AWS monitoring tools are used to assist in forensic analysis and to ensure proper containment and follow-up actions.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	If a threat is detected, access to affected systems is immediately restricted, and patches or configuration changes are applied to prevent further spread. Any compromised data or systems are isolated for analysis and remediation.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	After each incident, lessons learned are reviewed and documented internally. Where applicable, detection rules, access controls, and team procedures are updated to reduce the likelihood of similar incidents occurring in the future.
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	We maintain cloud-based backup and recovery processes to ensure minimal disruption in the event of a cybersecurity incident. Key assets and configurations can be restored using platform-native tools such as Azure Backup or AWS Backup, depending on the deployment.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Recovery procedures are reviewed after incidents to identify process gaps or delays. We adjust recovery scripts, automation tools, and team roles as needed based on post-incident evaluations.
	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).	In the recovery phase, relevant stakeholders—including the EA—are kept informed of system restoration timelines and actions taken. Internal communications are handled via assigned leads, and external parties are notified when required.







MentalUP_RSU14WindhamRaymond_ME_14State_OHG_vendorsigned

Final Audit Report

2025-12-08

Created:	2025-11-12
By:	TEC SDPA (bbirdsall@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAIx7g8hfFnYdxQny7iqKVKPgs4Q-PjskQ

"MentalUP_RSU14WindhamRaymond_ME_14State_OHG_vendorsigned" History

-  Document created by TEC SDPA (bbirdsall@tec-coop.org)
2025-11-12 - 5:50:00 PM GMT
-  Document emailed to Mike Duffy (mduffy@rsu14.org) for signature
2025-11-12 - 5:50:17 PM GMT
-  Email viewed by Mike Duffy (mduffy@rsu14.org)
2025-11-12 - 8:17:49 PM GMT
-  Email viewed by Mike Duffy (mduffy@rsu14.org)
2025-12-08 - 6:52:27 PM GMT
-  Document e-signed by Mike Duffy (mduffy@rsu14.org)
Signature Date: 2025-12-08 - 6:53:51 PM GMT - Time Source: server
-  Agreement completed.
2025-12-08 - 6:53:51 PM GMT