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

Pilgrim Area Collaborative

and

Rediker Software, Inc.

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between: Pilgrim Area Collaborative, located at 42 Industrial Park Rd, Plymouth, MA 02360 USA (the "**Local Education Agency**" or "**LEA**") and Rediker Software, Inc., located at 2 Wilbraham Road, Hampden, MA 01030 (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: ___John Cooper_____Title: ___Director of IT_____

Address: ___2 Wilbraham Road, Hampden, MA 01036_____

Phone: ___(413)462-9373_____Email: ___jcooper@rediker.com_____

The designated representative for the LEA for this DPA is:

Kelly McKende Director of Technology

6 Resnik Road, Suite 115, Plymouth MA 02360

781-296-6111   kmckende@pilgrimac.org

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

Pilgrim Area Collaborative

By: _Dympna Thomas (Nov 17, 2025 10:46:11 EST)_____ Date: ___11/17/2025_____

Printed Name: ___Dympna M. Thomas_____ Title/Position: ___Executive Director_____

Rediker Software, Inc.

By: _John Cooper_____ Date: ___11/13/2025_____
        John Cooper (Nov 13, 2025 08:26:36 EST)

Printed Name: ___John Cooper_____ Title/Position: ___Director of IT_____

3

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.

6

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

Student Information System
Rediker Software's Administrator's Plus® is a cloud-based PK-12 student information system that helps educators manage student data, attendance, student behavior, report cards, master schedule building, billing, notifications and more. Administrator's Plus is seamlessly integrated with the TeacherPlus web gradebook and the ParentPlus web portal, creating an integrated, secure online solution for school management. Mobile apps make it easy for administrator's, parents and students to access information.

Admissions & Enrollment
Rediker Software provides school admissions and enrollment solutions for all types of PK-12 schools. AdmissionsPlus makes it easy for any schools to track and communicate with each applicant step by step through the entire admissions process, from initial inquiry through acceptance and enrollment. AdmissionsPlus offers unique features for charter schools to bring applications online, conduct school lotteries and manage wait lists. Public schools and districts can streamline the re-enrollment process, making it faster and easier for parents and school staff.

Integrations & Partnerships
Integration, interoperability and partnership development with leading K-12 education companies; We partner with a growing list of education and technology providers to better support the needs of your entire K-12 school community. Browse our list of integrations and partnerships to learn more.

Evaluations & Walkthroughs
Teacher Evaluator is an affordable, web-based application that can be accessed through a dedicated iPad® app and any web browser. Evaluating staff can be a challenging task for any school. Each school has a unique approach with different requirements. No matter what SIS you have for your private school, public school, district or diocese, Teacher Evaluator has the tools you need to schedule and complete evaluations quickly, effectively and unobtrusively.

District & Diocesan Management
Public school districts and catholic diocese can manage the data for all schools in one easy-to-use solution. System-wide statistics, enrollments and transfers are part of our District or Diocesan School Management. Dashboards make it easy to view and analyze statistical information at a glance.

Responsive School Websites
Respond to the mobile requirements of prospects, parents and students. Responsive school websites from Rediker are optimized to make browsing easy for different devices, from desktop monitors to tablets and smartphones. With a school or district website hosted by Rediker Software, your school can have a great-looking, professional website that is mobile-friendly and easy to edit.

School Data Analytics
Creating data driven insights to improve decision making. The LiveBook comparative analytics technology is a platform to visualize data, explore relationships and associate content. Quickly see patterns, differences, ranks, trends, and linkages in data. Apply this knowledge to visualize, analyze, and understand your data leading to better decision making for evidenced based solutions.

Payment Services
We offer a better, faster payment processing will help save schools time and money, and is integrated with Admissions, AdminPlus Online Forms and RediSite school websites.

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:	X
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	X
	Student class attendance data	X
Communications	Online communications captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	X
Demographics	Date of Birth	X
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, or primary language spoken by student)	X
	Other demographic information-Please specify: *As required by State or Local entities; User defined*	X
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	X
	Specific curriculum programs	X
	Year of graduation	X
	Other enrollment information-Please specify: *Categorizations*	X
Parent/Guardian Contact Information	Address	X
	Email	X
	Phone	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	X
Parent/Guardian Name	First and/or Last	X

Category of Data	Elements	Check if Used by Your System
Schedule	Student scheduled courses	X
	Teacher names	X
Special Indicator	English language learner information	X
	Low income status	X
	Medical alerts/ health data	X
	Student disability information	X
	Specialized education services (IEP or 504)	X
	Living situations (homeless/foster care)	X
	Other indicator information-Please specify: *Military, gifted, lunch, after school programs*	X
Student Contact Information	Address	X
	Email	X
	Phone	X
Student Identifiers	Local (School district) ID number	X
	State ID number	X
	Provider/App assigned student ID number	X
	Student app username	X
	Student app passwords	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)	X
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
Student Survey Responses	Student responses to surveys or questionnaires	X
Student work	Student generated content; writing, pictures, etc.	X
	Other student work data -Please specify:	
Transcript	Student course grades	X
	Student course data	X
	Student course grades/ performance scores	X
	Other transcript data - Please specify:	X
Transportation	Student bus assignment	X
	Student pick up and/or drop off location	X

Category of Data	Elements	Check if Used by Your System
	Student bus card ID number	X
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application: *250 custom user defined fields for school specific data capture*	X
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

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

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

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

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, <u>et</u>. <u>seq</u>., R.I.G.L. 16-104-1, and R.I.G.L., 11-49.3 <u>et</u>. <u>seq</u>.; 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.

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

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

All policies provided via email.
_____

INFORMATION SECURITY PROGRAM AND POLICIES SUMMARY

Title: Information Security Program and Policies Summary

Department: IT   **Version:** 2.3

Author: John Cooper   **Approval date:** 11/30/2023

Approved by: John Cooper   **Effective date:** 1/1/2024

Senior management approval: **Last updated:** 6/6/2025

Policy Statement

This Information Security Policy includes information security requirements and acceptable use while operating within the organization's technology environment. Rediker Software, Inc. is dedicated to protecting employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet browsing, and FTP, are the property of Rediker Software, Inc. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations.

Effective security is a team effort involving the participation and support of every Rediker workforce member who deals with information and/or information systems. Every employee plays a role in securing data used for Rediker Software, Inc. internal functions as well as all data pertaining to and contained by a client's usage of Rediker Software, Inc. products. This document provides a high-level overview of Rediker Software, Inc.'s security-related IT practices, procedures and regulations.

Information Security Program

Each employee should be familiar with their role in the Rediker Software, Inc. Information Security Program. These requirements contain, but are not limited to:

1. Minimizing the collection and storage of sensitive information.

2. Limiting access to sensitive information to those who require it.

3. Education on data handling procedures and security awareness.

4. Utilization of secure practices and technologies.

5. Individual responsibility for accessing and securing data based on their role.

Applicability

This policy applies to the Rediker workforce. The workforce includes Rediker employees, contractors, and vendors who operate within the Rediker environment.

Scope

This policy applies to the use of information, electronic and computing devices, and network resources to

conduct Rediker business or interact with internal networks and business systems. This policy applies to all Rediker Software, Inc. workforce members, including employees, contractors, consultants, temp workers, and other workers at Rediker Software, Inc., including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Rediker Software, Inc. All workforce members at Rediker Software, Inc. and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Rediker Software, Inc. policies and standards, and local laws and regulations.

General Use and Ownership

1. Rediker Software, Inc. proprietary information stored on electronic and computing devices whether owned or leased by Rediker Software, Inc., the employee or a third party, remains the sole property of Rediker Software, Inc.

2. Employees have a responsibility to promptly report the theft, loss or unauthorized disclosure of Rediker Software, Inc. proprietary information.

3. You may access, use or share Rediker Software, Inc. proprietary information to the extent it is authorized and necessary to fulfill your assigned job responsibilities/

4. Workforce members are responsible for exercising good judgment regarding the reasonableness of personal use of Rediker Software, Inc. computer technology and it should not interfere with their job responsibilities. If personal use of Rediker Software, Inc. technology for personal use is deemed to be excessive, an individual may have their access restricted.

5. For security and network maintenance purposes, authorized individuals within Rediker Software, Inc. may monitor workforce member equipment use systems and network traffic at any time.

6. Rediker Software, Inc. reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of Rediker Software, Inc. authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Rediker Software, Inc. owned computer systems and technology. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Rediker Software, Inc.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Rediker Software, Inc. or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting Rediker Software, Inc. business is prohibited.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)

5. Revealing or sharing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Accessing a server, technology, or account that the workforce member is not expressly authorized to access to cause a disruption, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

7. Making fraudulent offers of products, items, or services originating from any Rediker Software, Inc. account.

8. Port scanning or security scanning is by individuals outside the security team.

9. Executing any form of network monitoring which will intercept data not intended for the workforce member's host.

Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. The following activities are prohibited:

1. Sending unsolicited email messages outside of job responsibilities, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Unauthorized use, or forging, of email header information.

3. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4. Creating or forwarding "chain letters", "Ponzi" or "pyramid" schemes of any type

5. Use of unsolicited email originating from within Rediker Software, Inc.'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Rediker Software, Inc. or connected via Rediker Software, Inc.'s network.

6. Posting the same or similar non-business-related messages to large numbers of users.

7. Personal postings and submissions by workforce members from a Rediker Software, Inc. email address to newsgroups, blogs, social media, or other Internet venues is prohibited. Exceptions are for postings and engagement for legitimate and approved business purposes

Data Classification

Rediker Software, Inc. classifies data based on three tiers:

Tier 1 (Public): Information that has been approved for release to the general public. This may include marketing material, information displayed on the Rediker Software, Inc. website, and public job postings.

Tier 2 (Internal): Internal information is not public and is intended for use only at Rediker Software, Inc. Unauthorized disclosure or access of "Internal" information is not likely to result in an adverse impact on customers, staff, or result in financial harm. Examples of internal data may include policies and standards, work schedules, and routine memos.

Tier 3 (Confidential): Confidential information is not to be disclosed to anyone without a specific need to know. Unauthorized disclosure or access to confidential information may result in significant harm to customers, employees, or financial harm to the organization. Examples of confidential data include financial information, PII, board minutes, PCI data, contracts and legal documents, and ITS IDs and passwords.

Applications that hold Confidential data must have user access reviews conducted annually. In addition, all permissions to Confidential data must be configured as minimum necessary and need to know basis only and granted based on an employee's job responsibilities.

Client Data

Client data pertaining to and contained by client's usage of Rediker Software, Inc. products must only be stored in storage directly controlled by Rediker Inc. Examples include network drives, Azure Cloud services, and other in-house data repositories. Client data should not be stored on personal devices, portable storage devices, or cloud services not managed by the Rediker Software, Inc.

Sensitive Information

Sensitive or confidential information must be protected against unauthorized access or public disclosure. Some examples include but are not limited to: Social Security numbers, passwords, credit card numbers, grades, bank account numbers, health information, biometric data (such as fingerprints) and disability status. It is the duty of everyone who handles sensitive information to prevent unauthorized disclosure and ensure regulatory compliance regardless of format.

Protecting Sensitive Information

Ensure that sensitive information is only disclosed to the people authorized to receive such information. When dealing with the public, you must verify the identity of an individual before making a transaction on their behalf or before disclosing sensitive information.

Sending and Receiving Sensitive Information

Rediker Software, Inc. employees and agents have a responsibility to protect Confidential and Sensitive Information (CSI). Transfer of CSI should only occur under specific circumstances where the transfer is appropriate, authorized, and secure**.**

If you come across a circumstance that requires you to send or receive CSI or PII, first verify the data transfer is appropriate. The following items should be considered:
- Is the receiving party authorized to receive the information? For example, a FERPA or similar release is on file with Rediker Software, Inc.
- Does the entity or party receiving the data have a legitimate reason to receive the data?
- Have you sufficiently verified the identity of the entity with whom you are working?
- Are all the data elements or fields required? If not, reduce the data to only those items required.
- If you do not know the answers, check with your supervisor.

If the data transfer is appropriate, check with your supervisor to determine if your department or organizational unit has an existing process in place. If not, seek guidance from IT.

Processing Sensitive Information

CSI must not be entered, pasted, uploaded, or otherwise submitted into unapproved externally controlled data processing, transformation, conversion or similar systems, including generative AI systems such as ChatGPT or online/cloud document conversion systems, such as PDF converters. These systems may subject CSI to unauthorized disclosure.

Approved Storage of Sensitive Information

Sensitive digital information should only be stored on an approved, access-controlled storage location. Some examples include departmental drives, Azure Cloud services, or other approved and access-controlled storage. Client data may only be stored within Azure Cloud services or within secured on-site servers. These locations are required to have protective controls to protect against unauthorized access.

Rediker Software, Inc. uses Microsoft Azure Cloud services to maintain both Rediker Software, Inc. and client data. Microsoft provides Azure customers with detailed information about security and compliance programs, including audit reports and compliance packages, to help customers assess our services against their own legal and regulatory requirements.
- ISO 27001/27002, SOC 1/SSAE 16/ISAE 3402 and SOC 2, Cloud Security Alliance CCM
- Fed RAMP, FISMA, PCI DSS Level 1
- HIPAA, FERPA, FIPS 140-2, CCCPPF, MLPS

More information on specific compliance programs is available here:
http://azure.microsoft.com/en-us/support/trust-center/

Rediker Software, Inc. maintains onsite datacenter in Hampden, MA. The server room, designed and constructed expressly for the purpose, is accessible only to specific individuals, and all instances of access to the room are logged.

Workstation hard drives may not be used to store sensitive or client information. Neither removable media (such as DVDs, CDs and flash drives) nor personal computing devices may be used to store sensitive information.

Clean Desk

Maintaining a clean desk is an important tool to ensure that no confidential materials are visible on a user's workspace. Confidential materials must be secured when the items are not in use, or an employee leaves his/her workstation. This is an important control to reduce the risk of security incidents or data leakage in the workplace.

Requirements

Employees are required to ensure that all confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

1. Computer workstations must be locked when the employee leaves their workspace.

2. Computer workstations must be shut down at the end of the workday.

3. Any Confidential information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

4. File cabinets containing Confidential information must be kept closed and locked when not in use or when not attended.

5. Keys used for access to Confidential information must not be left at an unattended desk.

6. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

7. Printouts containing Confidential information should be immediately removed from the printer.

8. Confidential documents should be shredded in shred bins.

9. Whiteboards containing Confidential information should be erased.

Ensure mass storage devices such as USBs or external drives are secure and not accessible when the workspace is unoccupied.

Information Handling and Electronic Communication

Rediker Software, Inc. requires that the handling and electronic communication of data be done in a secure manner using approved methods. All workforce members at Rediker Software, Inc. who handle and transmit Rediker Software, Inc. data must use discretion and operate on the principle of minimum necessary and only send data that is required to accomplish work objectives. To minimize data leakage, and ensure that data integrity is in place, Rediker Software, Inc. permits data transmission and communication by the following approved methods:

1. Email - company email can be used to transmit all data internally. Confidential data sent via email should be limited to the minimum necessary for business purposes. Only corporate email is permitted.

2. Text – text may be used for communication and sending non-confidential data.

3. Instant message – the following approved and adopted instant message communication methods may be used:

    3.1. Microsoft Teams

    3.2. Slack

    3.3. WhatsApp

4. Collaborative communications – Screen sharing type of communication among teams is restricted to the following approved and adopted applications:

    4.1. Microsoft Teams

    4.2. Zoom

5. Any other type of electronic communication methods not listed must be approved by senior management prior to usage. If non-approved methods of communication are used without express written permission, it may result in disciplinary action, up to, and including termination.

Email Security

Email is a critical means of communication both internally as well as with clients. Following the proscribed protocols will provide both Rediker Software, Inc. and our customers with data security.

Emailing Sensitive Information

Email should not be used to send sensitive information unless the sensitive information is encrypted using a business approved solution. Alternative options to sending sensitive information via email are available; IT should be contacted for assistance.

Phishing

Phishing is one of the most common ways attackers use to steal login information. An email is crafted which constructs a scenario designed to get the recipient to give out his or her username/password or other sensitive information. In some cases, the information is requested via email by impersonating IT support. IT support will never request a user's username or password. In other cases, a link is provided in the email which directs recipients to a fake but realistic-looking login site from which the credentials are harvested.

Always **Hover to Discover** to see where an email link leads before clicking. You can do this by "hovering" the mouse cursor over a link without clicking. The box that appears will show you where the link leads. This will help you to identify malicious websites before you click.

Should you accidentally respond to a phishing email, immediately change your password and contact the IT department at TechDesk@Rediker.com.

If you suspect a message is phishing, report it by sending it to TechDesk@Rediker.com. Create a new, blank message and add the phishing message as an attachment. This preserves header information for investigation.

The IT department will randomly send simulated phishing emails to random individuals as part of the

Rediker Software, Inc. security policy. These should be treated as real phishing attempts ad reported as such.

Laptops and Mobile Devices

All mobile and computing devices that connect to the internal network must comply with the Rediker Software, Inc. security policy requirements.

Business Laptops

Laptops provided by Rediker Software, Inc. are configured with full disk encryption using BitLocker. This includes a pre-boot password – a code that must be entered before the device will boot into Windows. The pre-boot password should never be recorded and stored with the laptop. Although full disk encryption provides a strong level of security, there are certain scenarios where this level of protection is insufficient. I f a laptop is on when it was lost, the encryption might not be sufficient since the information is decrypted while running. To protect against this vulnerability, turn the device off when not in use.

Laptops should be stored in a secure, locked location when not in use. When traveling, use the hotel safe if you leave it in your hotel room. Laptops may not be checked in luggage but instead must be transported as a carry-on item.

Whenever using a network not controlled by the Rediker Software, Inc., only the IT supplied VPN should be used. No other form of access is allowed.

Mobile Devices

Personally owned mobile devices, such as smart phones and tablets, can be used to connect to the Rediker Software, Inc. communication systems. This includes, but is not limited to email, Microsoft Teams, and Slack. The email app used must enforce Microsoft Exchange policies. The mobile device may also be used to maintain an MFA authenticator. The mobile device must lock after a period of inactivity, and may be unlocked using either PIN, pattern, or biometrics.

Using Free Wi-Fi While Traveling

Only connect to trusted wireless networks. Before using wireless networks outside of home or work, such as at a business or hotel, inquire about the official name of the wireless network before connecting. Doing so will reduce the risk of connecting to a malicious network which might attempt to steal information or infect your device.

International Travel

If you intend on accessing Rediker Software, Inc. computing resources while traveling abroad, you should contact the IT helpdesk at HelpDest@Rediker.com to discuss options for securely remote work. When returning to the United States, it is required to change any passwords have used while traveling.

Lost Laptops/Mobile Devices

Should you lose your laptop or mobile device, promptly report it the local police and notify IT by contacting the IT helpdesk at HelpDest@Rediker.com.

Home Office Connectivity for Business Devices

Employees working remotely that use Rediker Software, Inc. supplied hardware and connect to the internet must:

1. Enable WPA2 or WPA3 security on your home Wi-Fi network.
2. Passwords used to secure their network must follow the established password policy.
3. Always use the provided a virtual private network (VPN) when connecting to the Rediker Software, Inc. network for an additional layer of security.

Office Wi-Fi (Wireless Networks) access

Personal devices may access Rediker Software, Inc. provided wireless access using the guest network.

Remote Access from Personally Owned Devices

No remote access to the Rediker Software, Inc. environment is permitted.

Passwords

Your passwords are what protects your accounts from unauthorized access. Users are required to follow the guidelines set forth in the Rediker Software, Inc. Password Policy documentation.

Multi-Factor Authentication (MFA)

Access to some Rediker Software, Inc. resources may require Multi-Factor Authentication (MFA) upon login. This can be a phone call, text message, code from a mobile app, or notification to a mobile app. If you ever receive unexpected MFA calls, messages, or prompts, someone might be trying to get into your account. Should this occur to you, change your password and notify the IT helpdesk immediately at HelpDesk@Rediker.com.

Security Controls

Do not attempt to circumvent or disable Rediker Software, Inc. security controls. Examples to avoid include using proxy servers or third-party VPN services to bypass filtering or using hardware devices or software to prevent workstations from locking due to inactivity. No unauthorized applications may be installed on hardware belonging to Rediker Software, Inc.

Reporting Suspicious Activity

Data breaches are becoming more prevalent, requiring heightened vigilance to prevent their occurrence. If you

Information Security Program and Policies Summary v2.3

suspect a security incident or see unusual activity, please report it promptly by contacting the IT helpdesk at TechDesk@Rediker.com.

Suspicious Phone Calls

Should you receive a suspicious phone call where an unexpected caller asks you to take action on your computer or reveal sensitive information, do not follow their instructions or provide information. This may be a phone scam or a social engineering attack. Instead, report it to your supervisor or the IT helpdesk at TechDesk@Rediker.com. See <u>Reporting Security Incidents</u> section above for contact information.

Suspicious Emails

If you receive a suspicious email, do not follow any links or open any attachments. Instead, follow the reporting information in the <u>Phishing</u> section to report the message.

Suspicious SMS/Text Messages

Threat actors will use multiple means to compromise their targets. One method they use is SMS text messages on personal devices. Since these are outside of the Rediker Software, Inc. environment, the security tools used by Rediker Software, Inc. are not able to block or other detect these attacks. Should you receive a text message from an unknown individual requesting any Rediker Software, Inc. or client information, contact your supervisor or IT helpdesk at TechDesk@Rediker.com

Personal Anonymizing Services, such as Personal VPN, TOR, etc.

Do not use anonymizing services designed to obscure identity and location. This makes account activity look suspicious, and it is difficult to verify account activity as legitimate. Use of these services may prevent access or result in a suboptimal experience, such as unexpected logouts or other undesirable experiences. Examples include anonymizing VPNs like NORD VPN, or other services like TOR or web proxies.

Vulnerability Management

It is the policy of Rediker Software, Inc. to conduct periodic vulnerability assessment via vulnerability scanning to detect weaknesses that may be exploited by threats and to mitigate and address those vulnerabilities in the technology environment. The following are required:

1. Periodic and/or continuous vulnerability assessment scans will be performed on all network assets deployed on Rediker Software, Inc. IP address space.

2. Security vulnerabilities will be identified using industry-recognized sources for security vulnerability information.

3. Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.

4. Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.

5. All system components are protected from known vulnerabilities by installing applicable security

patches/updates. Patches/updates for critical vulnerabilities are installed within one month of release.

Regulation and Compliance

Rediker Software, Inc. is subject to several regulations based on the activities it performs and the information it holds. Each employee must handle data appropriately to comply with these regulations.

FERPA

The Family Educational Rights and Privacy Act of 1974 (FERPA) sets forth requirements designed to protect the privacy of student education records. FERPA provides for the right to inspect and review education records, the right to seek to amend those records and to limit disclosure of information from the records. FERPA applies to all institutions receiving funds under any program administered by the Secretary of Education.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a standard for organizations that accept credit cards. It places several requirements for security management, policies, procedures, network architecture, software design and other critical protective measures for systems that handle credit card data. Anyone who handles credit card data or transactions must be certain to protect this data and follow the PCI Data Security procedure. To meet the Payment Card Industry's Data Security Standards (DSS), the following security controls are required:

1. No PCI card holder data can be electronically or physically stored or retained. This includes the Cardholder's Primary Account Number (PAN), and any sensitive 3 or 4-digit data CAV2/CVC2/CVV2/CID or PIN.

2. The Cardholder's name can be stored along with expiration data so long as the PAN is not stored.

3. Any vendor default account used related to credit card payments must have their default password changed. If any vendor accounts will not be used, the account is removed or disabled.

4. Any allowable account data that is stored will only be retained for a 3-year period after which time it will be permanently deleted.

5. Vulnerability scanning will be completed quarterly for all PCI assets.

Additional regulations

- Usage of technologies and methodologies consistent with the guidance issued in the American Recovery and Reinvestment Act of 2009, Public Law 111-5, § 13402(h)(2), 42 U.S.C. § 17932.
- The Children's Online Privacy Protection Act of 1998 (COPPA) is a United States federal law, located at 15 U.S.C. §§ 6501–6506 (Pub. L. 105–277 (text) (PDF), 112 Stat. 2681-728, enacted October 21, 1998). We do not collect any information from anyone under 13 years of age. Our website, products and services are all directed to people who are at least 13 years old or older.

- The Children's Internet Protection Act (CIPA).
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Maintaining technical safeguards relating to the possession of education records in a manner consistent with 45 C.F.R. 164.312.
- Connecticut House Bill 7207 as amended by Public Act 16-189, and by Public Act 17-200, which is to be in force on and after July 1, 2018.
- HITECH (the Health Information Technology for Economic and Clinical Health Act of 2009) and the regulations thereunder (including 45 C.F.R. Sections 164.308, 164.310, 164.312, and 164.316)
- Usage of industry standard encryption and security protocols in compliance with Massachusetts 201 CMR 17.0 and Executive Order 504 (aka WISP legislation pertaining to confidentiality of student data).

Policy Compliance

1. The IT team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

2. Any exception to the policy must be approved by the Infosec team in advance.

Policy Noncompliance

Rediker Software, Inc. employees and authorized contractors who do not comply with this policy and the procedures that may be developed from it are subject to possible disciplinary measures as may be determined by Rediker Software, Inc.'s general counsel and/or human resources.

Questions

Should you have a question related to information security, please contact your supervisor or email the IT department at TechDesk@Rediker.com.

Rediker_PilgrimCollab_MA_14State_OHG (1) (1)

Final Audit Report 2025-11-13

Created:	2025-11-12
By:	TEC SDPA (mmcgrath@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA_S0NB0inoEWFRPrMo-JyqD-ja2UElcU_

"Rediker_PilgrimCollab_MA_14State_OHG (1) (1)" History

Document created by TEC SDPA (mmcgrath@tec-coop.org)
2025-11-12 - 6:49:29 PM GMT

Document emailed to jcooper@rediker.com for signature
2025-11-12 - 6:49:43 PM GMT

Email viewed by jcooper@rediker.com
2025-11-13 - 1:21:07 PM GMT

Signer jcooper@rediker.com entered name at signing as John Cooper
2025-11-13 - 1:26:34 PM GMT

Document e-signed by John Cooper (jcooper@rediker.com)
Signature Date: 2025-11-13 - 1:26:36 PM GMT - Time Source: server

Agreement completed.
2025-11-13 - 1:26:36 PM GMT

Rediker_PilgrimCollab_MA_14State_OHG (1) (1) - signed_final

Final Audit Report   2025-11-17

Created:	2025-11-14
By:	TEC SDPA (mmcgrath@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAdvMYGL3NX1ElOHtFX6I7RsAU3TIawf8a

"Rediker_PilgrimCollab_MA_14State_OHG (1) (1) - signed_final" History

Document created by TEC SDPA (mmcgrath@tec-coop.org)
2025-11-14 - 4:20:49 PM GMT

Document emailed to Kelly McKende (kmckende@pilgrimac.org) for signature
2025-11-14 - 4:21:07 PM GMT

Email viewed by Kelly McKende (kmckende@pilgrimac.org)
2025-11-17 - 3:39:29 PM GMT

Document signing delegated to Dympna Thomas (dthomas@pilgrimac.org) by Kelly McKende (kmckende@pilgrimac.org)
2025-11-17 - 3:40:27 PM GMT

Document emailed to Dympna Thomas (dthomas@pilgrimac.org) for signature
2025-11-17 - 3:40:28 PM GMT

Email viewed by Dympna Thomas (dthomas@pilgrimac.org)
2025-11-17 - 3:44:06 PM GMT

Document e-signed by Dympna Thomas (dthomas@pilgrimac.org)
Signature Date: 2025-11-17 - 3:46:12 PM GMT - Time Source: server

Agreement completed.
2025-11-17 - 3:46:12 PM GMT

Adobe Acrobat Sign