

**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**

**Erie 1 Board of Cooperative Educational Services**

**and**

**eDynamic Holdings LP**

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: Erie 1 BOCES, located 355 Harlem Road, West Seneca, NY 14224 USA (the “**Local Education Agency**” or “**LEA**”) and eDynamic Holdings LP, located at 221 River Street, Hoboken, NJ 07030 USA (the “**Provider**”).

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

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

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

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

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

The designated representative for the Provider for this DPA is:

Name: Brian Piccioni Title: Chief Financial Officer

Address: 221 River Street, Hoboken, NJ 07030

Phone: 877-585-2029 Email: proposals@edynamiclearning.com

The designated representative for the LEA for this DPA is:

Michelle Okal-Frink, Director  
355 Harlem Road West Seneca, NY 14224  
mokal@e1b.org 716-821-7200

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

**Erie 1 BOCES**

By: James Fregelette Date: 11/16/2025

Printed Name: James Fregelette Title/Position: Executive Director

**eDynamic Holdings LP**

By: E-SIGNED by Brian Piccioni  
on 2025-10-07 19:08:39 GMT  
B. L. Piccioni Date: October 07, 2025

Printed Name: Brian Piccioni Title/Position: Chief Financial Officer

## **STANDARD CLAUSES**

Version 3.0

### **ARTICLE I: PURPOSE AND SCOPE**

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

### **ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS**

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the

Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

### ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

### ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

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

## **ARTICLE V: DATA PROVISIONS**

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit “F”**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit “F”**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
- (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
    - i. The name and contact information of the reporting LEA subject to this section.
    - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
    - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
    - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
    - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
  - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
  - (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
  - (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
  - (5) In the event of a breach originating from LEA’s use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

## ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

## ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of



all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

**EXHIBIT "A"**  
**DESCRIPTION OF SERVICES**

**eDynamic Learning** - career and Technical Education (CTE) and online digital courseware.

**EXHIBIT "B"**  
**SCHEDULE OF DATA**

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

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

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

## **EXHIBIT “C”**

### **DEFINITIONS**

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

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

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

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

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

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

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

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

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

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

records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

**Subprocessor:** For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

**Subscribing LEA:** An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

**Targeted Advertising:** means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

**Third Party:** The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

**EXHIBIT "D"**  
**DIRECTIVE FOR DISPOSITION OF DATA**

**[Insert Name of District or LEA]** Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

\_\_\_\_\_ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

**[Insert categories of data here]**

\_\_\_\_\_ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

\_\_\_\_\_ Disposition shall be by destruction or deletion of data.

\_\_\_\_\_ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

**[Insert or attach special instructions]**

3. Schedule of Disposition

Data shall be disposed of by the following date:

\_\_\_\_\_ As soon as commercially practicable.

\_\_\_\_\_ By **[Insert Date]**

4. Signature

\_\_\_\_\_  
Authorized Representative of LEA

\_\_\_\_\_  
Date

5. Verification of Disposition of Data

\_\_\_\_\_  
Authorized Representative of Company

\_\_\_\_\_  
Date



**EXHIBIT “F”**  
**DATA SECURITY REQUIREMENTS**

**Adequate Cybersecurity Frameworks**  
**2/24/2020**

Cybersecurity Frameworks

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

**EXHIBIT "G"**  
**Massachusetts**

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

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

**EXHIBIT "G"**  
**Maine**

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

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
  - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
  - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
  - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

**EXHIBIT “G”**  
**Illinois**

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

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Illinois;

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

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

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

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

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

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

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

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

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

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

as a result of the security breach; and

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

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

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

**EXHIBIT “G”**  
**Iowa**

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

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Iowa;

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

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Iowa does not require all Student Data to be stored within the United States.
4. In Exhibit “C” add to the definition of “Student Data” significant information on progress and growth, experiences, interests, aptitudes, attitudes, abilities, part-time employment, and future plans.



## **EXHIBIT “G”**

### **Missouri**

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

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Missouri;

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

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Missouri does not require data to be stored within the United States.
4. Replace Article V, Section 4(1) with the following:
  - a. In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student’s family member, Provider shall notify LEA within seventy-two (72) hours. The notice shall include:
    - i. Details of the incident, including when it occurred and when it was discovered;
    - ii. The type of personal information that was obtained as a result of the breach; and
    - iii. The contact person for Provider who has more information about the incident.
  - b. “*Breach*” shall mean the unauthorized access to or unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person employed by or contracted with, or an agent of, Provider is not a breach provided that the personal information is not used in violation of applicable Federal or Missouri law, or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.
  - c. “*Personal information*” is the first name or initial and last name of a student or a family member of a student in combination with any one or more of the following data items that relate to the student or a family member of the student if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology such that the name or data elements are unreadable or unusable:
    - i. Social Security Number;
    - ii. Driver’s license number or other unique identification number created or collected by a government body;
    - iii. Financial account information, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
    - iv. Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
    - v. Medical information; or
    - vi. Health insurance information.

**EXHIBIT “G”**  
**Nebraska**

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

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Nebraska;

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

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

**EXHIBIT “G”**  
**New Jersey**

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

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Jersey;

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

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. The Provider will not disclose on its web site any personally identifiable information about a student, including, but not limited to student names, student photos, student addresses, student e-mail addresses, student phone numbers, and locations and times of class trips.
4. The Provider will not process Student Data in violation of State and federal laws that prohibit unlawful discrimination.
5. The Provider will not conduct processing that presents a heightened risk of harm to students without conducting and documenting a data protection assessment of each of its processing activities that involve Student Data.
6. In Article V, Section 1 Data Storage: New Jersey does not require data to be stored within the United States.
7. Add to the definition in Exhibit “C” of Student Data: “The location and times of class trips.”

## **EXHIBIT "G"**

### **Ohio**

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

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Ohio;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. In Article IV, Section 3, add: "The Provider will restrict unauthorized access by Provider's employees or contractors not providing services under the Service Agreement or DPA and its employees or contractors will only access Student Data as necessary to fulfill their official duties."
3. In Article IV, Section 6, replace "Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice," with "Upon termination of this DPA, unless the LEA provides notice that renewal of the contract is reasonably anticipated, within ninety (90) days of the expiration of the contract, Provider shall destroy or return Student Data to the LEA."
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Ohio does not require data to be stored within the United States.
6. Provider will not access or monitor any of the following:
  - a. Location-tracking features of a school-issued device;
  - b. Audio or visual receiving, transmitting or recording features of a school-issued device;
  - c. Student interactions with a school-issued device, including, but not limited to, keystrokes and web-browsing activity

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

**EXHIBIT “G”**  
**Rhode Island**

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

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

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

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
  - i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:
    1. The credit reporting agencies
    2. Remediation service providers
    3. The attorney general
  - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
  - iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student’s ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student’s requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

**EXHIBIT "G"**  
**Tennessee**

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

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Tennessee;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Tennessee does not require data to be stored within the United States.
4. The Provider agrees that it will not collect any individual student biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking.
5. The Provider agrees that it will not collect individual student data on:
  - a. Political affiliation;
  - b. Religion;
  - c. Voting history; and
  - d. Firearms ownership

## **EXHIBIT "G"**

### **Vermont**

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

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

**EXHIBIT “G”**  
**Virginia**

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

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Virginia;

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

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Virginia does not require data to be stored within the United States.
4. In Article V, Section 4, add: In order to ensure the LEA’s ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within twenty-four (24) hours, where the Provider reasonably expects or confirms Student Data may have been disclosed in a data breach.



**EXHIBIT "G"**  
**New Hampshire**

**WHEREAS**, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Hampshire. Specifically, those laws are RSA 189:1-e and 189:65-68-a; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

**WHEREAS**, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

**WHEREAS**, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Hampshire;

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

1. All references in the DPA to "Student Data" shall be amended to state "Student Data and Teacher Data." "Teacher Data" is defined as at least the following:

Social security number.  
Date of birth.  
Personal street address.  
Personal email address.  
Personal telephone number  
Performance evaluations.

Other information that, alone or in combination, is linked or linkable to a specific teacher, paraprofessional, principal, or administrator that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify any with reasonable certainty.

Information requested by a person who the department reasonably believes or knows the identity of the teacher, paraprofessional, principal, or administrator to whom the education record relates.

"Teacher" means teachers, paraprofessionals, principals, school employees, contractors, and other administrators.

2. In order to perform the Services described in the DPA, the LEA shall provide the categories of Teacher Data described in the Schedule of Data, attached hereto as **Exhibit "I"**.
3. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
4. In Article IV, Section 7 amend each reference to "students," to state: "students, teachers,..."
5. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
6. Provider is prohibited from leasing, renting, or trading Student Data or Teacher Data to (a) market or advertise to students, teachers, or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, teacher, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data and Teacher Data for the development of commercial products or services, other than as

necessary to provide the Service to the LEA. This section does not prohibit Provider from using Student Data and Teacher Data for adaptive learning or customized student learning purposes.

7. The Provider agrees to the following privacy and security standards. Specifically, the Provider agrees to:
  - (1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;
  - (2) Limit unsuccessful logon attempts;
  - (3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;
  - (4) Authorize wireless access prior to allowing such connections;
  - (5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;
  - (6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;
  - (7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;
  - (8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;
  - (9) Enforce a minimum password complexity and change of characters when new passwords are created;
  - (10) Perform maintenance on organizational systems;
  - (11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;
  - (12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1;
  - (13) Protect (i.e., physically control and securely store) system media containing Student Data or Teacher Data, both paper and digital;
  - (14) Sanitize or destroy system media containing Student Data or Teacher Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;
  - (15) Control access to media containing Student Data or Teacher Data and maintain accountability for media during transport outside of controlled areas;
  - (16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

- (17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;
- (18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);
- (19) Protect the confidentiality of Student Data and Teacher Data at rest;
- (20) Identify, report, and correct system flaws in a timely manner;
- (21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;
- (22) Monitor system security alerts and advisories and take action in response; and
- (23) Update malicious code protection mechanisms when new releases are available.

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

- 8. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:
  - i. The estimated number of students and teachers affected by the breach, if any.
- 9. The parties agree to add the following categories into the definition of Student Data: the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number.
- 10. In Article V, Section 1 Data Storage: New Hampshire does not require data to be stored within the United States.

**EXHIBIT "I" – TEACHER DATA**

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	<b>X</b>
	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, European Union, 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**

LEA's Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy for this service agreement can be accessed at:

[https://sdpc.a4l.org/ny\\_dp\\_bor\\_url.php?districtID=13045](https://sdpc.a4l.org/ny_dp_bor_url.php?districtID=13045)

**Exhibit “K”**  
**Provider Security Policy**

Provider’s Data Security and Privacy Plan can be accessed at

<https://www.edynamiclearning.com/privacy-policy/>

---

# DATA PRIVACY AND SECURITY PLAN

## Provider DATA PRIVACY AND SECURITY PLAN

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

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	<p>Over the life of the Contract, at eDynamic Learning, we are committed to implementing applicable data security and privacy contract requirements to safeguard sensitive information and protect the privacy of all parties involved. Our approach focuses on proactive measures, continuous monitoring, and periodic assessments to ensure compliance with the contract's data security and privacy provisions. Below is an outline of how we will achieve this:</p> <ol style="list-style-type: none"><li>1. Initial Compliance Assessment: At the start of the Contract, we conduct a thorough review of the data security and privacy requirements outlined in the agreement. This assessment includes identifying specific obligations and controls that need to be in place to meet contractual obligations and legal requirements.</li><li>2. Risk-Based Approach: We adopt a risk-based approach to prioritize areas of concern and allocate resources effectively. By assessing the potential risks associated with data processing and storage, we can focus on mitigating the most significant threats to data security and privacy.</li><li>3. Security and Privacy Policies and Procedures: We establish comprehensive security and privacy policies and procedures aligned with the contract's requirements. These documents serve as guidelines for employees and relevant stakeholders on how to handle, process, and protect sensitive data throughout the Contract's duration.</li><li>4. Data Classification and Handling: We classify data based on its sensitivity level, ensuring that appropriate security measures are applied to protect each category of data. This approach allows us to allocate resources based on the importance and criticality of the data being processed.</li><li>5. Access Control and Authorization: We implement strict access controls to limit data access to authorized personnel only. Role-based access and authentication mechanisms are employed to ensure that data can only be accessed by those with a legitimate need.</li><li>6. Data Encryption: All sensitive data, both in transit and at rest, is encrypted using industry-standard encryption algorithms. Encryption adds an extra layer of protection, making it significantly more challenging for unauthorized individuals to access the data.</li><li>7. Regular Security Training and Awareness: We conduct periodic security training and awareness programs for all employees and</li></ol>
---	--	--

		<p>subcontractors involved in the Contract. These initiatives promote a culture of security-consciousness and help ensure that everyone understands and adheres to data security and privacy best practices.</p> <p>8. Continuous Monitoring and Incident Response: We implement advanced monitoring tools to detect any potential security breaches or unauthorized access in real-time. If any incidents occur, we have a well-defined incident response plan in place to promptly address and mitigate the impact.</p> <p>9. Vendor Management and Subcontractor Oversight: If subcontractors are involved, we enforce contractual obligations on data security and privacy to ensure they adhere to the same level of protection as required by the main Contract. Regular assessments of subcontractors' compliance are conducted.</p> <p>10. Periodic Audits and Assessments: We conduct regular audits and assessments to evaluate the effectiveness of our data security and privacy measures. These reviews help us identify areas for improvement and ensure that we remain compliant with the contract's requirements.</p> <p>11. Documented Compliance Records: Throughout the Contract's life, we maintain detailed records of our compliance efforts, including security measures implemented, training records, incident responses, and audits. These records serve as evidence of our commitment to data security and privacy.</p> <p>12. Contract Renewals and Revisions: As the business landscape and data protection regulations evolve, we regularly review and update the Contract to incorporate any necessary changes. This ensures that the data security and privacy provisions remain relevant and effective. By implementing these measures over the life of the Contract, we aim to foster a secure and trustworthy environment, maintaining the confidentiality and integrity of sensitive data while meeting all applicable data security and privacy requirements throughout our engagement.</p>
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	<p>At eDynamic Learning, the protection of Personally Identifiable Information (PII) is of paramount importance to us. We have implemented a comprehensive set of administrative, operational, and technical safeguards and practices to ensure the utmost security and privacy of PII. Below is an overview of the safeguards and practices we have in place:</p> <p>1. Administrative Safeguards:</p> <ul style="list-style-type: none"> <li>• Data Governance and Policies: We have established clear data governance frameworks and policies that outline the handling, processing, and storage of PII. These policies govern how employees and relevant stakeholders must interact with PII to maintain confidentiality and integrity.</li> <li>• Access Control and Authorization: Access to PII is strictly controlled through role-based access mechanisms. Employees are granted access to PII on a need-to-know basis, and permissions are regularly reviewed and updated.</li> </ul>

		<ul style="list-style-type: none"> <li>• Employee Training and Awareness: All employees undergo comprehensive training on data security, privacy practices, and the importance of protecting PII. We regularly conduct awareness programs to keep our workforce informed about the latest security threats and best practices.</li> <li>• Incident Response and Management: We have a well-defined incident response plan in place to handle any potential security breaches or incidents involving PII. This plan includes predefined procedures for reporting, investigation, containment, and mitigation of such incidents.</li> </ul> <p>2. Operational Safeguards:</p> <ul style="list-style-type: none"> <li>• Data Minimization: We follow the principle of data minimization, ensuring that we only collect and retain the minimum amount of PII necessary to fulfill our contractual or legal obligations.</li> <li>• Data Retention Policies: PII is retained only for the required duration, as specified in our data retention policies. Once the retention period expires, we securely delete the data.</li> <li>• Secure Document Handling: PII in physical form is stored securely and access is restricted to authorized personnel only. We maintain secure storage facilities with restricted access to protect physical records.</li> <li>• Third-Party Risk Management: When third-party vendors are involved in processing PII, we conduct thorough assessments to ensure they meet the same high standards of data security and privacy protection.</li> </ul> <p>3. Technical Safeguards:</p> <ul style="list-style-type: none"> <li>• Data Encryption: PII is encrypted both in transit and at rest using industry-standard encryption algorithms. This ensures that even if unauthorized access occurs, the data remains unreadable and unusable.</li> <li>• Firewalls and Intrusion Detection Systems: We employ firewalls and intrusion detection systems to protect our network from unauthorized access and potential cyber threats.</li> <li>• Multi-Factor Authentication (MFA): To enhance the security of user accounts, we implement MFA, which requires multiple forms of authentication before granting access to sensitive data or systems.</li> <li>• Regular Security Updates and Patches: We proactively monitor and apply security updates and patches to our systems and software to prevent vulnerabilities that could be exploited.</li> </ul> <p>These administrative, operational, and technical safeguards and practices collectively form a robust and layered approach to protecting PII at eDynamic Learning. We continuously evaluate and enhance our security measures to stay ahead of emerging threats and ensure the highest level of data security and privacy for our customers, partners, and employees.</p>
--	--	---

3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	We conduct periodic security training and awareness programs for all employees and subcontractors involved in the Contract. These initiatives promote a culture of security-consciousness and help ensure that everyone understands and adheres to data security and privacy best practices.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	<p>At eDynamic Learning, we place great importance on ensuring that all parties involved in our contracts, including employees and subcontractors, are bound by written agreements that adhere to the requirements of the Contract, at a minimum. Our contracting processes are designed to create a legally binding framework that enforces compliance with contractual obligations and fosters a strong commitment to data security and privacy. Here is an outline of how we achieve this:</p> <ol style="list-style-type: none"> <li>1. Contract Review and Approval: Before engaging in any contractual relationship, our legal and procurement teams meticulously review and draft the contract to include all necessary requirements. This includes specific provisions that detail the obligations of employees and subcontractors in meeting the Contract's stipulations.</li> <li>2. Clear Definitions and Scope: The contract explicitly outlines the roles, responsibilities, and deliverables of all parties involved. By clearly defining the scope of work, each party understands its obligations, making it each to ensure compliance.</li> <li>3. Incorporation of Data Security and Privacy Requirements: Data security and privacy are paramount in our contracting processes. We ensure that the contract includes clauses that mandate strict adherence to applicable data protection laws and confidentiality requirements.</li> <li>4. Confidentiality and Non-Disclosure Agreements: In cases where sensitive information or proprietary data is shared, we execute confidentiality and non-disclosure agreements with employees and subcontractors. These agreements legally bind all parties to maintain the confidentiality of shared information.</li> <li>5. Oversight and Compliance Management: Throughout the contract's duration, we maintain oversight to ensure all parties are complying with the contract's provisions. Regular assessments and audits help identify areas for improvement and ensure continuous compliance.</li> <li>6. Monitoring and Incident Response: We implement monitoring tools to detect potential breaches or unauthorized access to data. In the event of any incidents, we have well-defined incident response procedures to address and mitigate the impact promptly.</li> <li>7. Vendor Management and Subcontractor Obligations: When subcontractors are involved, we ensure they sign agreements with data security and privacy requirements consistent with the primary contract. Regular evaluations of subcontractors' compliance are conducted.</li> <li>8. Documented Records and Retention: All contractual agreements, including confidentiality and non-disclosure agreements, are securely stored and retained as per our document retention policies. This ensures access to relevant information during compliance checks or disputes.</li> <li>9. Contract Renewals and Updates: As</li> </ol>

		<p>business needs evolve or regulations change, we regularly review and update the contract to incorporate necessary revisions. This ensures that the contract remains relevant and up-to-date with the latest data security and privacy requirements.</p> <p>By following these contracting processes, we aim to establish a robust legal framework that binds all parties involved to the requirements of the Contract. This approach ensures that our employees and subcontractors understand their obligations, fostering a culture of compliance and data protection throughout our engagements. The result is a strong commitment to data security and privacy that aligns with our dedication to responsible business practices.</p>
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	<p>At eDynamic Learning, we take data security and privacy incidents very seriously, especially when they involve Personally Identifiable Information (PII). Our approach to managing such incidents is comprehensive and designed to ensure the protection of sensitive data and compliance with relevant regulations. Below, we outline our strategies for handling data security and privacy incidents that implicate PII, as well as our plans for identifying breaches and unauthorized disclosures and reporting incidents to the appropriate authorities, such as the Customer (regulatory body or relevant organization).</p> <ol style="list-style-type: none"> <li>1. Incident Response Team: We have a dedicated Incident Response Team composed of skilled professionals from various departments, including IT, legal, compliance, and management. This team is responsible for swiftly addressing and resolving any data security and privacy incidents.</li> <li>2. Incident Identification and Monitoring: We employ advanced monitoring and detection systems to identify potential breaches or unauthorized access to PII. These systems continuously analyze network activity, logs, and other data sources, allowing us to detect anomalies or suspicious activities promptly.</li> <li>3. Breach Notification Plan: In the event of a data breach that involves PII, we have a well-defined breach notification plan. This plan outlines the necessary steps to assess the scope and impact of the breach, contain it, and notify affected individuals and relevant authorities within the required time frames.</li> <li>4. Communication Protocols: Effective communication is crucial during data security incidents. Our Incident Response Team maintains clear communication channels with all stakeholders, including customers, employees, partners, and regulatory bodies. Transparent and timely communication helps build trust and ensures that everyone is informed about the incident's status and measures being taken.</li> <li>5. Legal and Compliance: We work closely with legal and compliance experts to ensure that our incident response actions align with local and international data protection laws and regulations. This includes adhering to reporting requirements and providing the necessary documentation to the customer and other relevant authorities.</li> <li>6. Data Minimization and Encryption: To reduce the potential impact of a breach, we follow data minimization principles, only collecting and retaining essential PII. Additionally,</li> </ol>



		<p>sensitive data is encrypted both in transit and at rest to protect it from unauthorized access.</p> <p>7. Employee Training and Awareness: We invest in regular training and awareness programs to educate our employees about data security best practices and privacy policies. By fostering a culture of security awareness, we empower our workforce to become the first line of defense against potential incidents.</p> <p>8. Regular Security Audits and Assessments: We conduct frequent security audits and risk assessments to identify vulnerabilities and proactively address potential weaknesses in our systems and processes. This allows us to stay ahead of emerging threats and continually improve our security measures.</p> <p>9. Continuous Improvement: Our incident response and data security policies are not static. We regularly review and update our procedures based on lessons learned from previous incidents and industry best practices. By implementing these strategies, we aim to maintain the highest level of data security and privacy protection, swiftly address any incidents that arise, and fulfill our obligations to report incidents to the customer and other relevant authorities as required. Safeguarding our customers' and stakeholders' data remains at the forefront of our commitment to responsible data management.</p>
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	<p>At eDynamic Learning, we understand the importance of responsible data management, including the secure transition of data to the customer when it is no longer needed to meet our contractual obligations. Our data transition process is carefully planned and executed to ensure the privacy and integrity of the data throughout the transfer. Here is a description of how we handle the data transition:</p> <p>1. Data Retention Policies: We establish data retention policies that specify the duration for which we will retain the data in accordance with contractual requirements and relevant legal obligations. Once the data is no longer needed to fulfill our contractual obligations, we initiate the data transition process.</p> <p>2. Data Inventory and Categorization: Before transitioning the data, we conduct a thorough inventory and categorization of the information. This step helps us identify and segregate sensitive data, such as PII, proprietary information, or any other confidential data that requires special handling during the transition.</p> <p>3. Secure Data Deletion: For data that is no longer required and does not need to be transferred to the customer, we employ secure data deletion methods, following industry best practices and standards. This process ensures that data is irreversibly removed from our systems and storage devices.</p> <p>4. Data Anonymization or Aggregation: In some cases, the customer may require certain data for statistical analysis or reporting purposes without directly identifying individuals or organizations. In such instances, we anonymize or aggregate the data to protect individual privacy while still providing valuable insights.</p> <p>5. Data Transfer Agreements: When transitioning data to the customer, we establish written agreements that outline the terms of the transfer, including the scope of data, data format,</p>

		<p>security requirements, and the purpose of the data's use by the customer. These agreements ensure a clear understanding of the responsibilities and obligations of both parties during the transition.</p> <p>6. Data Security during Transfer: We employ secure data transfer methods, such as encrypted channels, to ensure the confidentiality and integrity of the data during the transition process. This prevents unauthorized access or interception of the data while it is in transit.</p> <p>7. Validation and Verification: Before completing the data transition, we validate and verify the accuracy and completeness of the transferred data. This step ensures that the customer receives the necessary information and that the data is in compliance with the agreed-upon format and specifications.</p> <p>8. Data Deletion Confirmation: For data that is deleted or no longer needed</p> <p>9. Our commitment to data security and privacy extends throughout the entire data lifecycle, including the data transition process. By following these procedures, we ensure that data is managed responsibly and ethically, meeting our contractual obligations while safeguarding the privacy and confidentiality of the information.</p>
7	Describe your secure destruction practices and how certification will be provided to the EA.	<p>Here's an overview of our secure deletion:</p> <p>1. Secure Deletion Methods: We utilize approved methods for secure data deletion. Our IT team oversees this process to ensure the thorough and effective removal of data.</p> <p>2. Chain of Custody: To maintain the integrity of data deletion, we maintain a clear chain of custody for storage media that contains sensitive data. This chain of custody ensures that the data remains under controlled access until it is securely destroyed.</p> <p>3. Data Deletion Policy Communication: We maintain open and transparent communication with the customer about our data deletion policies and procedures. This ensures that the customer is aware of the measures we take to safeguard data during and after the contract period.</p> <p>By adhering to these secure deletion practices to the customer, we demonstrate our commitment to protecting sensitive data and maintaining reasonable level of data security. Our processes are designed to instill confidence in the customer that the data entrusted to us has been handled responsibly and securely throughout its lifecycle, upholding our dedication to data privacy and protection.</p>
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	<p>At eDynamic Learning, our data security and privacy program/practices are designed to align seamlessly with the customer's applicable policies and requirements. We recognize the significance of adhering to the customer's guidelines and regulations to protect sensitive information and maintain the confidentiality and integrity of data. Below is an outline of how our data security and privacy program/practices align with the customer's policies:</p> <p>1. Compliance with customer's Data Security and Privacy Standards:</p> <ul style="list-style-type: none"> <li>We conduct a thorough analysis of the customer's data security and privacy policies and standards to ensure a comprehensive</li> </ul>

		<p>understanding of their requirements.</p> <ul style="list-style-type: none"> <li>• Our data security and privacy program is designed to incorporate the customer's standards as the foundation for our own policies and practices.</li> </ul> <p>2. Data Classification and Handling:</p> <ul style="list-style-type: none"> <li>• We classify data based on the customer's guidelines to appropriately determine the level of protection required for each data category.</li> <li>• Our data handling procedures are aligned with the customer's recommendations, ensuring that sensitive information is treated with the utmost care and security</li> </ul> <p>3. Access Controls and Authorization:</p> <ul style="list-style-type: none"> <li>• We implement access controls in accordance with the customer's guidelines, ensuring that data is only accessible to authorized personnel.</li> <li>• Role-based access mechanisms are employed to restrict access to data based on job responsibilities, following the customer's principles of least privilege.</li> </ul> <p>4. Data Encryption:</p> <ul style="list-style-type: none"> <li>• Our data encryption practices are aligned with the customer's recommendations, using industry-standard encryption protocols to protect data both in transit and at rest.</li> <li>• Encryption is applied to sensitive information to ensure it remains secure and confidential, as outlined in the customer's data protection policies.</li> </ul> <p>5. Incident Response and Reporting:</p> <ul style="list-style-type: none"> <li>• Our incident response plan aligns with the customer's requirements for reporting and addressing data security incidents.</li> <li>• We promptly notify the customer of any data breaches or incidents, ensuring compliance with their incident reporting procedures.</li> </ul> <p>6. Third-Party Management:</p> <ul style="list-style-type: none"> <li>• Our vendor and subcontractor management practices adhere to the customer's guidelines, ensuring that any third parties involved in data processing meet the same security and privacy standards.</li> <li>• We require third-party service providers to sign agreements that comply with the customer's data security and privacy requirements.</li> </ul> <p>7. Data Retention and Deletion:</p> <ul style="list-style-type: none"> <li>• Our data retention and deletion policies are in line with the customer's recommendations to ensure data is retained only for as long as necessary and securely disposed of when no longer needed.</li> <li>• We provide certification of data deletion nto the customer, confirming that data has been securely removed when required.</li> </ul> <p>8. Auditing and Assessments:</p>
--	--	---

		<ul style="list-style-type: none"><li>• We conduct regular internal audits and assessments to verify that our data security and privacy practices remain in alignment with the customer's policies.</li></ul>
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

## EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Provider's Data Privacy and Security Plan. Provider should complete the Provider Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies ); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	<b>Asset Management (ID.AM):</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	<p>We conduct a comprehensive assessment of our data assets, systems, and processes to identify and classify sensitive information, including Personally Identifiable Information (PII).</p> <p>We establish and maintain an inventory of our data assets and categorize them based on their criticality and sensitivity levels.</p>
	<b>Business Environment (ID.BE):</b> The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Our organization's mission and objectives are clearly defined and well-communicated throughout the workforce. The cybersecurity strategy is aligned with these core principles to ensure that security measures contribute directly to the achievement of organizational goals.
	<b>Governance (ID.GV):</b> The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	<p>We maintain a data governance framework that defines roles and responsibilities for data security and privacy compliance across the organization.</p> <p>Our data security and privacy practices align with relevant regulatory requirements and industry standards.</p>
	<b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	<p>Regular risk assessments are conducted to identify potential vulnerabilities and assess the impact of threats on our data assets.</p> <p>We prioritize risks based on their severity and implement risk management strategies to address and mitigate identified vulnerabilities.</p>
	<b>Risk Management Strategy (ID.RM):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	In the security plan, attention is dedicated to delineating the organization's core priorities, operational constraints, risk tolerances, and underlying assumptions, forming a foundational framework that profoundly influences operational risk decisions. By articulating these elements, we create a nuanced understanding of the organization's strategic imperatives, limitations, and the level of risk acceptance. This clarity is pivotal in shaping and aligning operational risk decisions with the overarching business objectives. Through a dynamic interplay of these factors, the security plan ensures a responsive and adaptive approach, enabling the organization to navigate the complex landscape of operational risks with a tailored strategy that resonates with its unique priorities and risk appetite.

	<b>Supply Chain Risk Management (ID.SC):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	<p>In adherence to Supply Chain Risk Management (ID.SC) principles, our organization systematically establishes and leverages its priorities, constraints, risk tolerances, and assumptions to underpin informed risk decisions pertaining to supply chain management. This entails a comprehensive approach, wherein processes have been developed, implemented, and continuously refined to systematically identify, assess, and manage risks inherent in our supply chain. By aligning our risk management strategies with the organization's overarching priorities and risk appetite, we ensure a proactive and resilient stance against potential disruptions, fostering a robust supply chain that contributes to the overall resilience of our operations.</p>
Function	Category	Contractor Response
PROTECT (PR)	<b>Identity Management, Authentication and Access Control (PR.AC):</b> Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	<p>Access controls and authentication mechanisms are implemented to ensure that data is only accessible to authorized personnel based on the principle of least privilege.</p> <p>We employ data encryption techniques to protect sensitive data both in transit and at rest, in line with NIST encryption standards.</p> <p>Regular data backups and disaster recovery plans are in place to protect against data loss and enable data restoration when necessary.</p>
	<b>Awareness and Training (PR.AT):</b> The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	<p>We conduct regular security awareness training for all employees, contractors, and third-party vendors to enhance their understanding of data security best practices and privacy policies.</p> <p>Our workforce is educated about their roles and responsibilities in safeguarding data and preventing security incidents.</p>
	<b>Data Security (PR.DS):</b> Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	<p>In order to safeguard the confidentiality, integrity, and availability of information, eDynamic Learning adheres to a comprehensive security plan that aligns with our established risk strategy. By implementing robust security measures, such as access controls, encryption protocols, and regular audits, eDynamic strives to prevent unauthorized access, protect data from manipulation or corruption, and guarantee its accessibility when needed.</p>
	<b>Information Protection Processes and Procedures (PR.IP):</b> Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	<p>eDynamic Learning maintains a comprehensive set of policies to address purpose, scope roles and responsibilities and other aspects of protection of data, systems and assets. Those policies have owners, are regularly reviewed and updated and stored in our compliance system.</p>
	<b>Maintenance (PR.MA):</b> Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	<p>eDynamic Learning performs regular maintenance on its systems and system components. Maintenance scope and schedule is aligned with eDynamic security policies.</p>
	<b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	<p>The management of technical security solutions is a critical aspect of fortifying the security and resilience of systems and assets. This entails a comprehensive approach to overseeing and optimizing security measures, ensuring they align seamlessly with organizational directives. By consistently monitoring, updating, and fine-tuning these technical solutions, our organization effectively mitigates vulnerabilities and adapts to evolving threats, thereby upholding the overall integrity and robustness of our systems.</p>
	<b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected and the potential impact of events is understood.	<p>We deploy intrusion detection and prevention systems to monitor network activity and promptly detect any potential security breaches or suspicious activities.</p> <p>We implement robust logging and auditing mechanisms to track data</p>

DETECT (DE)		access and identify any unauthorized or anomalous behavior.
	<b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Our security plan includes processes and systems designed to detect intrusion and other security events. Those systems are monitored 24x7 by specialized teams and service providers.
	<b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Our security plan includes processes and systems designed to detect intrusion and other security events. Those systems are tested during annual penetration tests and monitored 24x7 by specialized teams/ services.
Function	Category	Contractor Response
RESPOND (RS)	<b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Our incident response plan outlines clear procedures for promptly responding to and mitigating data security incidents.  We conduct tabletop exercises and simulations to test the effectiveness of our incident response processes and ensure preparedness.
	<b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Our security plan emphasizes a holistic approach to response activities, ensuring seamless coordination with both internal and external stakeholders. Internally, our response teams collaborate closely with relevant departments, aligning efforts to address and mitigate the impact of security incidents. Externally, we establish communication channels with key partners to enhance our response capabilities.
	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	Our security plan incorporates a crucial phase of analysis to ensure the efficacy of our response efforts and provide robust support for subsequent recovery activities. Following the detection of any security incident, a comprehensive analysis is undertaken to understand the nature, scope, and potential impact of the event. This analysis informs the fine-tuning of our response strategies, enabling us to tailor our actions to the specific characteristics of the incident. Moreover, the insights gained during this analysis phase play a pivotal role in supporting the recovery process by identifying areas for improvement and lessons learned. By maintaining a continuous feedback loop between analysis, response, and recovery, we not only enhance our incident management capabilities but also fortify our organization's resilience against future security challenges.
	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Our security plan adopts a comprehensive approach to incident management, encompassing proactive measures to prevent the expansion of events, mitigate their effects, and ultimately resolve incidents. Prevention strategies are implemented through robust security controls, threat intelligence integration, and regular vulnerability assessments. In the event of an incident, immediate actions are taken to contain and mitigate the impact, limiting potential damage and disruption. Our response framework focuses on a swift and efficient resolution, leveraging a combination of technical expertise, incident-specific playbooks, and continuous communication. By addressing incidents holistically, we aim not only to minimize immediate consequences but also to fortify our defenses against similar future threats, contributing to an overall resilient and adaptive security posture.
	<b>Improvements (RS.IM):</b> Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Our security plan underscores a commitment to perpetual enhancement of organizational response activities through a deliberate assimilation of lessons learned from both current and past detection/response endeavors. After each incident, a comprehensive analysis is conducted to identify areas of strength and improvement. These insights are systematically integrated into our response protocols, contributing to a more agile and adaptive approach. By applying knowledge learned from previous experiences, we fine-tune our detection and response strategies, bolstering the effectiveness of our security posture. This iterative process not only ensures a more resilient response to evolving threats but also fosters a proactive culture where the organization is constantly learning and evolving to stay ahead in the dynamic landscape of cybersecurity.

RECOVER (RC)	<p><b>Recovery Planning (RC.RP):</b> Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.</p>	<p>In the event of a data security incident, we have well- defined recovery procedures to restore affected systems and data to normal operations.</p> <p>Data restoration from backups is performed to recover lost or compromised information, minimizing the impact of an incident.</p>
	<p><b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.</p>	<p>Continuous enhancement of recovery planning and processes is ingrained in our cybersecurity strategy, with a focus on incorporating valuable lessons learned into future activities.</p> <p>Through rigorous post-incident analyses, we identify strengths and areas for improvement in our recovery procedures. These insights are systematically integrated into our recovery planning framework, ensuring that each incident becomes an opportunity for refining and strengthening our response capabilities. By leveraging lessons learned, we not only enhance the effectiveness of our recovery processes but also foster a culture of resilience, where adaptability and continuous improvement are foundational elements in our approach to cybersecurity. This commitment ensures that our organization remains agile and well-prepared to mitigate and recover from diverse cyber threats.</p>
	<p><b>Communications (RC.CO):</b> Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).</p>	<p>Our security plan emphasizes the importance of seamless coordination during restoration activities, both internally and externally. Internally, our incident response team collaborates closely with relevant departments, ensuring a cohesive approach to system restoration. Externally, coordination extends to key stakeholders. This effort is guided by established protocols and communication channels, facilitating the exchange of critical information and resources. By engaging with a network of trusted entities, we enhance our ability to expedite recovery processes, share threat intelligence, and collectively strengthen our cybersecurity posture. This approach ensures that restoration activities are not only efficient but also aligned with broader industry best practices and the evolving threat landscape.</p>







# eDynamicHoldings\_Erie1BOCES\_NY\_14State\_OHG\_VendorSigned

Final Audit Report

2025-11-16

Created:	2025-11-14
By:	TEC SDPA (mklisiwecz@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAfs8M3smhflwCKIIOgaTjMkVR-n1NbAF

## "eDynamicHoldings\_Erie1BOCES\_NY\_14State\_OHG\_VendorSigned" History

-  Document created by TEC SDPA (mklisiwecz@tec-coop.org)  
2025-11-14 - 6:28:25 PM GMT
-  Document emailed to James Fregelette (jfregelette@e1b.org) for signature  
2025-11-14 - 6:28:41 PM GMT
-  Email viewed by James Fregelette (jfregelette@e1b.org)  
2025-11-16 - 7:42:56 PM GMT
-  Document e-signed by James Fregelette (jfregelette@e1b.org)  
Signature Date: 2025-11-16 - 7:44:06 PM GMT - Time Source: server
-  Agreement completed.  
2025-11-16 - 7:44:06 PM GMT