

STANDARD STUDENT DATA PRIVACY AGREEMENT

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

MA-ME-IL-MO-NH-NY-OH-RI-TN-VT-VA-DPA, Modified Version 1.0

Medfield Public Schools

and

EDCLUB, INC

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: Medfield Public Schools, located at 459 Main Street, Third Floor, Medfield, MA 02052 USA (the “**Local Education Agency**” or “**LEA**”) and EdClub, Inc, located at 1701 Pennsylvania Ave. NW, Suite 200, Washington, DC 20006 (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. Only the Supplemental State Terms (if any) for the state of the applicable LEA shall apply.
 - 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: Mohsen Attarpour Title: Authorized Person

Address: 1701 Pennsylvania Ave. NW, Suite 200, Washington, DC 20006

Phone: 202-609-9919 Email: mohsen@edclub.com & support@edclub.com

The designated representative for the LEA for this DPA is:

Eoin Ocorcora, Director of Technology

459 Main Street, Third Floor, Medfield, MA 02052

508-242-8522

eocorcora@email.medfield.net

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

Medfield Public Schools

By: EOIN O'CORCORA Date: 09/02/2025

Printed Name: Eoin O'Corcora Title/Position: Director of Technology

EdClub, Inc

By: Mohsen Attarpour Date: 8/7/2025

Printed Name: Mohsen Attarpour Title/Position: Authorized Person

STANDARD CLAUSES

Version 3.0

ARTICLE I: PURPOSE AND SCOPE

- 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
- 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”**.
- 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

- 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.
- 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.
- 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.
- 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 and/or confidentiality policies for 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, 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 applicable law, including 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, 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 within 90 days. 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 received from the LEA or any portion thereof as it pertains to the delivery of services to the LEA. Any such audit shall be at no cost to Provider, excluding the Provider employee time, and shall be limited in scope to the LEA's services and data only. 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 of the LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the 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 reasonable 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 aspects of an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Provider's Information Security and Acceptable Use Policy has been provided to LEA prior to signing this DPA. 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 discovered 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 commercially reasonable and 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 and Provider's Terms of Service and Privacy Policy 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 would violate Federal, state or local law for the LEA to contract with the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it will enforce the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, on 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

Providing subscriptions to EdClub products as licensed. EdClub products include web-based education tools to teach users skills such as touch typing, digital citizenship, spelling and vocabulary (among others).

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: User agent	X
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify: Typing test	X
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	X
	Student grade level	X
	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	X
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	
	Provider/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	X
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	X
	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 that has not been de-identified, 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 "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
<input type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input type="checkbox"/>	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
<input 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, 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: “To the extent lawfully permissible: 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).” Current list of subcontractors is attached.
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 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.

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.

Application/Org name	Link to their Privacy Policy	Reason
Zendesk	https://www.zendesk.com/company/privacy	Organizing and handling Support Requests
Alchemer	https://www.alchemer.com/privacy/	Sending surveys to teachers and others if they opt in
Amazon Web Services	https://aws.amazon.com/agreement/	Hosting EdClub's videos
Atlantech.net	https://www.atlantech.net/privacy-policy	Hosting EdClub's servers and data analytics - private cloud
Coresite.com	https://www.coresite.com/privacy	Hosting EdClub's servers and data analytics - private cloud
Cloudflare	https://www.cloudflare.com/privacypolicy/	CDN, WAF, DDoS protection, DNS
Linode.com	https://www.akamai.com/legal/privacy-statement	SFTP
sentry.io	https://sentry.io/privacy/	Tracking errors on website
DataDog	https://www.datadoghq.com/legal/privacy/	Monitoring our performance metrics
MailChimp	https://mailchimp.com/legal/privacy/	Communicating feature releases with customers

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 of discovery. The notice shall include: (to the extent available)
 - 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"

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 or assisting with 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 of Provider's system, 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." Add: "as permitted under applicable law".
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 (to the extent available):
 - 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 "1" – TEACHER DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify: User agent	X
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: First and last name; email address; and Instructor ID (optional)	X

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 in Exhibit K and is incorporated into this DPA.
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 (via training procedures, informational documents and/or materials) 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 or assist with the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide or assist 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 required or permitted 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 pursuant to NY Executive Law § 63(15), 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 within ninety (90) days.

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a **“Directive for Disposition of Data”** form, a copy of which is attached hereto as **Exhibit “D”**, or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **“Exhibit D”**.

11. To amend Article IV, Section 7 to add: ‘Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, “which term shall not include students.”
12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
13. To add to Article V, Section 2 (Audits) the following:

To the extent required by law: 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. Provider’s Information Security and Acceptable Use Policy has been provided to LEA for review and approval prior to signing this DPA.

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 7 days 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 commercially reasonable and necessary to expeditiously secure Student Data.

(6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

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

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

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

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

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

Exhibit “J”
LEA Documents

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

Exhibit "K"
Provider Security Policy

Provider's Data Security and Privacy Plan is attached

EDCLUB, INC.
INFORMATION SECURITY AND ACCEPTABLE USE POLICY

1. Overview

All EdClub Information Systems that Employees use to carry out their job functions are the property of EdClub. Information Systems are to be used for business purposes in serving the interests of the company and our clients in the course of normal business operations.

Effective security is a team effort requiring the participation and support of every Employee who handles information and/or Information Systems. Every Employee is responsible for knowing, and conducting their activities in accordance with, this policy.

2. Purpose

The purpose of this policy is to establish rules governing the acceptable use of EdClub's Information Systems. These rules are designed to protect EdClub, its clients, and its Employees. Failure to adhere to this policy will expose EdClub, its clients, and its Employees to risks, including potential cybersecurity attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to all EdClub Employees and Information Systems. All EdClub Employees are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with EdClub policies and standards, as well as and local laws and regulations. Exceptions to this policy are documented in Section 5.2.

4. Policy

4.1 General Use and Ownership

- 4.1.1 EdClub Confidential Information stored on Information Systems remains the sole property of EdClub. Employees must ensure that Confidential Information is protected in accordance with the *Data Protection Standard*.
- 4.1.2 Employees have a responsibility to promptly report the theft, loss, or unauthorized access to or disclosure of EdClub proprietary information.
- 4.1.3 Employees may access, use, or share EdClub Confidential Information only to the extent it is authorized and necessary to fulfill their assigned job duties.
- 4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Information Systems. If there is any uncertainty, Employees should consult their supervisor or manager.
- 4.1.5 For security and network maintenance purposes, authorized Employees may monitor equipment, systems, and network traffic at any time, in accordance with the *Audit Policy*.
- 4.1.6 EdClub reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- 4.1.7 Employees must protect all Confidential Information, including by not sharing, posting, publishing, commenting on, or otherwise disclosing Confidential Information unless they are explicitly authorized to do so.

4.2 Security and Proprietary Information

- 4.2.1 Employees must use extreme caution when opening email attachments, which may contain malware. Even emails that appear to be sent by coworkers may be malicious. Upon receipt of an email that looks out of the ordinary or suspicious, Employees shall check with the sender before opening any attachments.
- 4.2.2 Employees must be alert for potential phishing attacks. Phishing is a type of attack usually carried out through malicious emails, in which the sender pretends to be a credible source and requests sensitive information. Attackers can set up web sites under their control that look and feel like legitimate web sites. Phishing emails often have an immediate call to action that ask the recipient to “update your account information” or “login to confirm ownership of your account.” Employees who suspect a phishing attack shall refrain from clicking on any links or opening any attachments, close the email, and report the situation to their supervisor immediately.

- 4.2.3 Employees shall not import any files that were created outside of EdClub's Information Systems into its Information Systems until those files are first scanned for viruses by an anti-virus program. Similarly, Employees shall not attach devices, including USB keys, to Information Systems unless they have prior approval.
- 4.2.4 All electronic devices that connect to Information Systems shall comply with the *Minimum Access Policy*.
- 4.2.5 System-level and user-level passwords shall comply with the *Password Policy*. Employees are prohibited from providing access to another individual, either deliberately or through failure to secure access.
- 4.2.6 All Information Systems shall be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Employees shall lock the screen or log off when the device is unattended.
- 4.2.7 Public communications by Employees that use an EdClub email address shall contain a disclaimer stating that the opinions expressed are strictly the Employees' own and not necessarily those of EdClub, unless posting is in the course of business duties.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of performing their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Any exemption from these restrictions must be approved by EdClub in writing before the conduct occurs.

Under no circumstances may an EdClub Employee engage in any activity that is illegal under local, state, federal, or international law while using Information Systems or Confidential Information.

The examples below are not exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- (a) Violations of the rights of any person or company protected by copyright, trade secret, patent, intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by EdClub. Employees shall not download software without the approval of a supervisor.

- (b) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources; or copyrighted music.
- (c) Accessing Information Systems for any purpose other than conducting EdClub business.
- (d) Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws. Employees must consult a supervisor before exporting regulated materials.
- (e) Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- (f) Revealing account passwords to non-Employees or allowing account access by others, including family and other household members.
- (g) Using Information Systems to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the Employee's local jurisdiction. Please see the *EdClub Employee Handbook* for additional information related to EdClub's policy against unlawful harassment.
- (h) Making fraudulent offers of products, items, or services originating from any EdClub account.
- (i) Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these activities are in the scope of normal job duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- (j) Port scanning or security scanning, unless prior written notification to EdClub has been made or these activities are part of the Employee's job function.
- (k) Executing any form of network monitoring that will intercept data not intended for the Employee's host, unless this activity is a part of the Employee's normal job function.
- (l) Circumventing user authentication or security of any host, network, or account.
- (m) Introducing honeypots, honeynets, or similar technology on Information Systems.
- (n) Using any program, script, or command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via Information Systems.
- (o) Providing information about, or lists of, EdClub Employees or customers to third parties outside EdClub.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, Employees must realize they represent the company.

The following activities are strictly prohibited, without exception:

- (a) Sending unsolicited email messages, including the sending of “junk mail” or other advertising material, to individuals who did not specifically request such material (email spam).
- (b) Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages. Employees may not send harassing, intimidating, offensive, abusive, threatening, menacing, or hostile content to anyone by any means.
- (c) Unauthorized use, or forging, of email header information.

3.1 Impersonating anyone else, whether inside or outside the company.

- (d) Creating or forwarding “chain letters,” “Ponzi” or other “pyramid” schemes of any type.

4.3.3 Social Media and Blogging

- (a) Employees are prohibited from using or accessing Social Media or blogging at work for non-EdClub-related reasons. Employees are not prohibited from using social media or blogging outside of work, but any posts, messages, videos, or pictures provided outside of work shall not be related to EdClub, its business practices, intellectual property, trade secrets, trademarks, logos, or other associated information.
- (b) Use of Social Media or blogging for EdClub-related reasons, whether using EdClub’s property and systems or personal computer systems, is subject to the terms and restrictions set forth in this policy. All EdClub-related online dialogue shall be conducted in a professional and responsible manner. Such dialogue shall not otherwise violate EdClub’s policies or be detrimental to EdClub’s best interests. Employees shall not engage in any dialogue that may harm or tarnish the image, reputation and/or goodwill of EdClub and/or any of its Employees. Use of Social Media or blogging from EdClub’s systems is also subject to monitoring.
- (c) EdClub’s *Data Protection Standard* also applies to social media and blogging. As such, Employees are prohibited from revealing any Confidential Information when engaged in Social Media or blogging.
- (d) When using Social Media or blogging, Employees are prohibited from making any discriminatory, disparaging, defamatory, or harassing comments or otherwise engaging in any conduct prohibited by EdClub’s policy against unlawful harassment. Please see the *EdClub Employee Handbook* for more information.

- (e) Employees may not attribute personal statements, opinions, or beliefs to EdClub when using Social Media or engaged in blogging. Unless authorized to speak on behalf of the company via Social Media, Employees shall never claim to speak on behalf of EdClub or express an official company position in such communications. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee shall not, expressly or implicitly, represent that he or she is representing EdClub's viewpoint. Employees assume any and all risks associated with blogging.
- (f) Employees will be held accountable for the information they share online. Any information shared, published, posted, or otherwise disclosed on the Internet should not adversely affect EdClub's image, reputation or good will. Employees are personally responsible for what they share, even if they attempt to modify or delete it. Should EdClub or its clients, agents or assigns suffer any adverse consequences based upon an Employee's violation of this Policy, EdClub reserves the right to hold that Employee fully accountable for its losses.

5. Policy Compliance

5.1 Compliance Measurement

EdClub will verify compliance with this policy through various methods, including but not limited to, business tool reports and internal and external audits. Employees learning of any misuse of Information Systems or violations of this policy must notify management immediately.

5.2 Exceptions

Nothing in this Information Security and Acceptable Use Policy is intended to limit, restrict, inhibit, or interfere in any way with an employee's right to discuss with others and/or post any workplace concerns including wages, hours, terms, and conditions of employment.

Any exception to the policy must be approved in writing by EdClub in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Glossary of Terms

Terms that are capitalized but not defined have the meanings assigned to them in applicable EdClub policies or procedures.

“Confidential Information” shall mean important or valuable business information that is not available to the public or personal information. Confidential information includes: Personal Information; customer information (personal, financial, and/or business information); internal policies and procedures of EdClub and/or its customers and vendors; product information; Employee information; marketing strategies; financial records or information; trade secrets or any other data that may be considered confidential.

“Data Breach” shall mean an event that causes or could cause the accidental, unauthorized, or unlawful destruction of, loss of, alteration of, disclosure of, or access to, Confidential Information.

“EdClub” or “company” shall mean EdClub, Inc., which includes, individually and collectively, EdClub and its affiliates.

“Employees” shall mean EdClub’s employees, officers, directors, contractors, consultants, temporary workers, and other workers at EdClub.

“Information Systems” shall mean EdClub’s network, accounts, and electronic devices, including Internet/Intranet/Extranet-related systems, computer equipment, mobile devices, licensed and developed software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP servers that EdClub purchases or leases for EdClub’s business purposes or that EdClub permits to access EdClub’s Information Systems, such as Employees’ personal mobile phones to the extent that Employees use such personal devices for EdClub’s business purposes.

“Personal Information” shall mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

“Social Media” shall mean web-based technologies used to broadcast messages and participate in dialogues. Examples of Social Media include social networking applications such as Facebook or MySpace; video-sharing applications such as YouTube; micro-blogging applications such as Twitter; collaboration applications such as Wikipedia; and EdClub’s internal networking tools.

EDCLUB, INC. DATA PROTECTION STANDARD

1. Overview

EdClub creates, receives, uses, and stores various data, including trade secrets and data about customers. It is the responsibility of every Employee to collect, protect, use, and disclose data only in accordance with this Data Protection Standard (“Policy”).

2. Purpose

This Policy establishes EdClub’s rules regarding data protection for Confidential Information.

3. Scope

This Policy applies to Employees and others who may have access to EdClub’s Information Systems.

4. Policy

4.1 Confidentiality of Confidential Information

- 4.1.1 EdClub invests substantial resources in creating and using various types of data. Improper use or disclosure of data could create legal risk for the Company and result in loss of a competitive advantage. All Confidential Information shall be protected against misuse, Data Breach, and improper or inadvertent disclosure, as described below.
- 4.1.2 These rules apply regardless of whether Confidential Information is stored electronically, on paper, or in any other medium.
- 4.1.3 Employees shall not use Confidential Information for private or commercial purposes, disclose it to unauthorized persons, or use or disclose it in any other unauthorized way. Supervisors shall inform their Employees at the start of the employment relationship about the obligation to protect Confidential Information. This obligation shall remain in force even after employment has ended. Confidential Information shall not be distributed, repurposed, or shared without authorization. For example, Confidential Information should not appear in URLs, error messages, or other public-facing data.
- 4.1.4 Personal Information shall only be collected to the extent that it is required for the specific purpose of which the data subject has been given notice. Any Personal Information that is not necessary for that purpose shall not be collected.

- 4.1.5 Confidential Information shall not be kept longer than is necessary for a legitimate business purpose. Such information shall be destroyed or erased from EdClub's systems when it is no longer required.
- 4.1.6 Private keys shall be kept confidential and protected, whether in transit or at rest. Keys shall be randomly chosen, and will allow for retrieval of information for administrative or forensic use.

4.2 Data Security

- 4.2.1 All Employees shall implement appropriate measures designed to ensure the confidentiality, security, and availability of Confidential Information.
- 4.2.2 Confidential Information shall be encrypted when in transit and at rest consistent with current best practices, such as the most recent National Institute for Standards and Technology ("NIST") guidelines.
- 4.2.3 Information Systems shall run operating systems and firmware currently supported by their developers. Operating systems shall be configured according to current best information security practices. Operating systems and firmware shall be kept current with the latest viable patches.
- 4.2.4 Devices capable of doing so shall have installed anti-virus software that shall be configured to run scheduled scans and to obtain the latest definitions as they become available. Anti-virus software shall be approved by management before use.
- 4.2.5 Upon termination of employment, Employees shall return all EdClub devices to EdClub, including mobile devices, laptops, USB keys, and physical media containing Confidential Information. As soon as possible after receiving devices back from Employees, and in any event before permitting another Employee to use the device, EdClub shall erase, destroy, and render unreadable all Confidential Information on the devices in its entirety in a manner that prevents its physical reconstruction through the use of commonly available file restoration utilities.
- 4.2.6 Employees shall participate in ongoing information security training approved by management.
- 4.2.7 Consistent with reasonable best practices, Employees shall implement a comprehensive secure development lifecycle system, including policies, training, audits, testing, emergency updates, proactive management, design reviews, code reviews, a change management process, and regular updates to the secure development lifecycle system itself.

4.2.8 Passwords shall be stored using a non-reversible, iterative, salted, one-way cryptographic hash.

5. Compliance

5.1 Compliance Measurement

EdClub will verify compliance with this Policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, and internal and external audits.

5.2 Exceptions

EdClub must approve any exceptions to the Policy in advance.

5.3 Non-Compliance

An Employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

Glossary of Terms

Terms that are capitalized but not defined have the meanings assigned to them in applicable EdClub policies or procedures.

“Confidential Information” shall mean important or valuable business information that is not available to the public or personal information. Confidential information includes: Personal Information; customer information (personal, financial, and/or business information); internal policies and procedures of EdClub and/or its customers and vendors; product information; Employee information; marketing strategies; financial records or information; trade secrets or any other data that may be considered confidential.

“Data Breach” shall mean an event that causes or could cause the accidental, unauthorized, or unlawful destruction of, loss of, alteration of, disclosure of, or access to, Confidential Information.

“EdClub” or “company” shall mean EdClub, Inc., which includes, individually and collectively, EdClub and its affiliates.

“Employees” shall mean EdClub’s employees, officers, directors, contractors, consultants, temporary workers, and other workers at EdClub.

“Information Systems” shall mean EdClub’s network, accounts, and electronic devices, including Internet/Intranet/Extranet-related systems, computer equipment, mobile devices, licensed and developed software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP servers that EdClub purchases or leases for EdClub’s business purposes or that EdClub permits to access EdClub’s Information Systems, such as Employees’ personal mobile phones to the extent that Employees use such personal devices for EdClub’s business purposes.

“Personal Information” shall mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

“Social Media” shall mean web-based technologies used to broadcast messages and participate in dialogues. Examples of Social Media include social networking applications such as Facebook or MySpace; video-sharing applications such as YouTube; micro-blogging applications such as Twitter; collaboration applications such as Wikipedia; and EdClub’s internal networking tools.

EDCLUB, INC. MINIMUM ACCESS POLICY

1. Overview

All devices connected to Information Systems shall comply with this Minimum Access Policy (the “policy”). Compliance with these requirements is further mandated by the *EdClub Information Security and Acceptable Use Policy*.

2. Purpose

The purpose of this policy is to maintain an adequate level of security to protect the confidentiality, availability, and integrity of Confidential Information and Information Systems. This policy defines the rules necessary to achieve this protection and to ensure the secure and reliable operation of Information Systems.

3. Scope

This policy applies to all devices connected to Information Systems, all Employees, and all personnel affiliated with third parties (collectively, “Users”) who have access to Information Systems. A written exception is required for any configuration that does not comply with this policy.

4. Policy

4.1 Minimum Access

- 4.1.1 Users shall be granted access to Information Systems and Confidential Information on a need-to-know basis. Users shall only receive access to the minimum applications and privileges required for performing their job duties.
- 4.1.2 Users are prohibited from gaining unauthorized access to any Information Systems or in any way damaging, altering, or disrupting the operation of these systems.
- 4.1.3 Information System access shall not be granted to any User without appropriate permissions.

4.2 Privileged Accounts

- 4.2.1 Privileged accounts used by administrators and other personnel with special permissions shall not be used for non-administrator activities. Network services shall run under accounts assigned the minimum necessary privileges.

4.3 Terminating User Access

4.3.1 Any changes in User duties or employment status shall be reported to appropriate managers. The affected User's access shall be immediately revoked if the User has been terminated. User access shall be appropriately modified if the User's work responsibilities have changed.

4.4 Use of Authentication

4.4.1 Information Systems shall require authentication by means of passphrases or other secure authentication mechanisms. Authentication requirements shall be appropriate to the type of data involved and transportation medium. EdClub shall use a third-party provider that is a recognized and trusted authority in the industry to generate any certificates used for authentication.

4.4.2 All network-based authentication shall be strongly encrypted. Traffic for one-time password authentication systems may be exempted from this encryption requirement. Users shall transmit Confidential Information only over TLS or via other secure methods, and shall use only SSL and similar technologies with appropriate safeguards in place.

4.4.3 Information Systems that are left unattended for more than 20 minutes shall be configured to log out automatically and require a User to re-authenticate. Information Systems that do not support an auto-log off function shall be secured with physical access restrictions.

4.4.4 Devices such as printers do not require authentication if the explicit purpose of the device is to provide unauthenticated access. Any devices that do not require authentication shall be physically secure and reasonable efforts shall be made to ensure that such devices are not readily accessible to unauthorized individuals.

4.5 Software Testing and Patch Updates

4.5.1 Devices connected to the EdClub network shall only run software for which timely security patches are available. All available security patches shall be applied according to a regular schedule that is appropriate for the confidentiality level of the affected data.

4.5.2 Confidential Information shall not be used in the development or testing of any products unless EdClub explicitly approves such use in writing beforehand and specific additional safeguards to protect such information are implemented.

4.6 Anti-Malware and Firewall Software

- 4.6.1 Anti-malware software shall be updated and running on Information Systems for which anti-malware software is available. Information Systems shall be scanned regularly for malware.
- 4.6.2 Host-based firewall software shall be running and configured to block all inbound traffic that is not explicitly required for the intended use of the Information System.

4.7 Information System Access Control Systems

- 4.7.1 All Information Systems used for EdClub business, regardless of where such systems are located, shall use an access control system approved by EdClub. In most cases this will involve password-enabled lock screens with an automatic log-off feature. Information Systems that are unlocked or unsecured shall not be left unattended for prolonged periods.
- 4.7.2 When a User leaves an Information System unattended, that User shall properly log out of all applications and networks. Users will be held responsible for all actions taken using devices or login credentials that are assigned to them.
- 4.7.3 Accounts will be locked after multiple failed login attempts. Affected Users shall be required to provide additional proof of identity to obtain access.

4.8 Confidential Information Access

- 4.8.1 Access to Confidential Information will be logged and audited in a manner that allows the following information to be deduced:
 - (a) Access time
 - (b) User account
 - (c) Method of access
 - (d) Privileged commands (which shall be traceable to specific User accounts)
- 4.8.2 All inbound access to EdClub's systems containing Confidential Information shall be logged. Audit results shall be securely stored and made available to the Data Breach Response Team in the event of any data breach.
- 4.8.3 Remote access to EdClub systems shall conform to this policy and shall comply with all applicable statutory requirements related to accessing and storing Confidential Information.

5. Policy Compliance

5.1 Compliance Measurement

EdClub will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, and internal and external audits.

5.2 Exceptions

Any exception to the policy must be approved by EdClub in advance.

5.3 Non-Compliance

A User found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Glossary of Terms

Terms that are capitalized but not defined have the meanings assigned to them in applicable EdClub policies or procedures.

“Confidential Information” shall mean important or valuable business information that is not available to the public or personal information. Confidential information includes: Personal Information, customer information (personal, financial, and/or business information); internal policies and procedures of EdClub and/or its customers and vendors; product information; Employee information; marketing strategies; financial records or information; trade secrets or any other data that may be considered confidential.

“Data Breach” shall mean an event that causes or could cause the accidental, unauthorized, or unlawful destruction of, loss of, alteration of, disclosure of, or access to, Confidential Information.

“EdClub” or “company” shall mean EdClub, Inc., which includes, individually and collectively, EdClub and its affiliates.

“Employees” shall mean EdClub’s employees, officers, directors, contractors, consultants, temporary workers, and other workers at EdClub.

“Information Systems” shall mean EdClub’s network, accounts, and electronic devices, including Internet/Intranet/Extranet-related systems, computer equipment, mobile devices, licensed and developed software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP servers that EdClub purchases or leases for EdClub’s business purposes or that EdClub permits to access EdClub’s Information Systems, such as Employees’ personal mobile phones to the extent that Employees use such personal devices for EdClub’s business purposes.

“Personal Information” shall mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

“Social Media” shall mean web-based technologies used to broadcast messages and participate in dialogues. Examples of Social Media include social networking applications such as Facebook or MySpace; video-sharing applications such as YouTube; micro-blogging applications such as Twitter; collaboration applications such as Wikipedia; and EdClub’s internal networking tools.

EDCLUB, INC.
PASSWORD CONSTRUCTION AND PROTECTION POLICY

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access to and/or exploitation of Information Systems and Confidential Information. All Employees and third parties with access to EdClub systems shall take the appropriate steps, outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

3. Scope

This policy applies to Employees and all personnel affiliated with third parties (collectively, “Users”) that have accounts that permit access to Information Systems. This policy applies to all passwords, including but not limited to user-level accounts, system-level accounts, web accounts, email accounts, screen saver protection, voicemail, and local router logins.

4. Policy

4.1 Password Creation

- 4.1.1 Users shall use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their personal accounts or vice versa.
- 4.1.2 User accounts that have system-level privileges shall be protected by a unique password that is different from the passwords for all other accounts maintained by that User to access system-level privileges.

4.2 Password Construction

4.2.1 Password Length

Longer passwords are more secure. All passwords on EdClub systems shall be at least 10 characters long. However, a password length of at least 14 characters is recommended.

4.2.2 Password Content

We highly encourage the use of passphrases (passwords made up of multiple words). Examples include “It’s time for vacation” or “block-curious-sunny-leaves.” These passphrases are easy to remember, easy to type, and improve account security.

Your password must include at least one special character or number. We encourage you to place these characters towards the middle of the password. Placing special characters or numbers only at the end of a password greatly reduces their effectiveness in thwarting security threats.

4.2.3 Unacceptable passwords

EdClub passwords shall not display any of the following characteristics:

- (a) Personal information, such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- (b) Sports or pop culture references.
- (c) Obvious character substitutions, such as substituting 3 for “e” or \$ for “s.”
- (d) Number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- (e) Variations of “Welcome123” “Password123” or “Changeme123.”

4.3 Password Protection

4.3.1 Passwords shall not be shared with anyone, including coworkers. All passwords shall be treated as Confidential Information.

4.3.2 Passwords shall not be inserted into email messages, shared via other types of electronic communication, or revealed over the phone to anyone.

4.3.3 Passwords may only be stored in “password managers” that are authorized by the organization.

4.3.4 Users may not use the "Remember Password" feature of web browsers or other applications.

4.3.5 Any User suspecting that his or her password may have been compromised shall report the incident to management and change the password.

4.4 Password Change

4.4.1 Passwords should only be changed when there is reason to believe a password has been compromised.

4.4.2 Password cracking or guessing may be performed on a periodic or random basis by EdClub. If a password is guessed or cracked during one of these scans, the User will

be required to change it to be in compliance with the Password Construction Guidelines.

4.5 Application Development

Application developers shall ensure that their programs contain the following security precautions:

- 4.5.1 Applications support authentication of individual Users, not groups.
- 4.5.2 Applications do not store passwords in clear text or in any easily reversible form.
- 4.5.3 Applications do not transmit passwords in clear text over the network.
- 4.5.4 Applications provide for some sort of role management, such that one User can take over the functions of another without having to know the other's password.

4.6 Multi-Factor Authentication

- 4.6.1 Multi-factor authentication is required for accounts with access to the Personal Information that EdClub processes on behalf of its clients, and highly encouraged for other work-related accounts and personal accounts also.

5. Policy Compliance

5.1 Compliance Measurement

EdClub will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, and internal and external audits.

5.2 Exceptions

Any exception to the policy must be approved by EdClub in advance.

5.3 Non-Compliance

A User found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Glossary of Terms

Terms that are capitalized but not defined have the meanings assigned to them in applicable EdClub policies or procedures.

“Confidential Information” shall mean important or valuable business information that is not available to the public or personal information. Confidential information includes: Personal Information; customer information (personal, financial, and/or business information); internal policies and procedures of EdClub and/or its customers and vendors; product information; Employee information; marketing strategies; financial records or information; trade secrets or any other data that may be considered confidential.

“Data Breach” shall mean an event that causes or could cause the accidental, unauthorized, or unlawful destruction of, loss of, alteration of, disclosure of, or access to, Confidential Information.

“EdClub” or “company” shall mean EdClub, Inc., which includes, individually and collectively, EdClub and its affiliates.

“Employees” shall mean EdClub’s employees, officers, directors, contractors, consultants, temporary workers, and other workers at EdClub.

“Information Systems” shall mean EdClub’s network, accounts, and electronic devices, including Internet/Intranet/Extranet-related systems, computer equipment, mobile devices, licensed and developed software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP servers that EdClub purchases or leases for EdClub’s business purposes or that EdClub permits to access EdClub’s Information Systems, such as Employees’ personal mobile phones to the extent that Employees use such personal devices for EdClub’s business purposes.

“Personal Information” shall mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

“Social Media” shall mean web-based technologies used to broadcast messages and participate in dialogues. Examples of Social Media include social networking applications such as Facebook or MySpace; video-sharing applications such as YouTube; micro-blogging applications such as Twitter; collaboration applications such as Wikipedia; and EdClub’s internal networking tools.

EDCLUB, INC. AUDIT POLICY

1. Overview

For security and network maintenance purposes, authorized Employees may monitor equipment, systems, and network traffic at any time. EdClub shall audit networks and systems in accordance with this Audit Policy (“Policy”).

2. Purpose

This Policy establishes EdClub’s rules regarding Audits. Audits are meant to verify that security controls are operating properly, a formal data protection system is in place, and all Employees are aware of and use that data protection system.

3. Scope

This Policy applies to all EdClub Employees and Information Systems.

4. Content of Audit

Audits shall occur at least once per year. Audits shall evaluate whether each element of EdClub’s information security policies is operating as intended. Audits may also address, but are not limited to, the following questions:

4.1 Data Origin and Storage

4.1.1 From whom is the Confidential Information collected? Confidential Information obtained from residents of certain jurisdictions may be subject to specialized regulatory regimes, such as the GDPR in the European Union or the CCPA in California.

4.1.2 Where is the Confidential Information stored? Is it held on the premises or in third-party data centers?

4.1.3 What information about EdClub’s data privacy and security practices has been disclosed to the source of the Confidential Information?

4.1.4 Have the purposes of the data collection been disclosed to the source of the Confidential Information?

4.2 Minimum Necessary Data

4.2.1 Has it been verified that the purposes of data collection could not be achieved effectively with less Confidential Information?

4.2.2 Is the Confidential Information being collected adequate to serve the stated purpose(s)?

4.3 Accuracy of Data

4.3.1 Have steps been taken to ensure the accuracy of the Confidential Information?

4.3.2 Is there a system of rolling reviews of Confidential Information to keep it up to date?

4.4 Data Retention

4.4.1 Is Confidential Information kept long enough to comply with relevant laws and regulations that define minimum data retention periods?

4.4.2 Is Confidential Information retained for longer than the minimum required retention period? If yes, is there a justification for doing so?

4.5 Appropriate Security Measures

4.5.1 Is the level of security adopted appropriate to the risks represented by the nature of the Confidential Information to be protected? Consideration should be given to the security of Confidential Information and the measures taken to guard against theft, computer viruses, or accidental disclosure.

4.5.2 Are Employees who handle Confidential Information aware of their responsibilities and obligations regarding that data?

4.5.3 Where consultants/contractors have access to Confidential Information, is there a data protection agreement in place that sets out the consultant's or contractor's data security obligations?

4.5.4 Are appropriate measures in place for the secure disposal and/or destruction of Confidential Information that is no longer required?

Glossary of Terms

Terms that are capitalized but not defined have the meanings assigned to them in applicable EdClub policies or procedures.

“Audit” means a systematic examination to determine whether activities involving the processing of Confidential Information are carried out in accordance with EdClub’s policies. Audits may be performed internally by authorized individuals within EdClub or externally by third parties authorized by EdClub.

“Confidential Information” shall mean important or valuable business or personal information that is not available to the public. Confidential information includes but is not necessarily limited to: customer information (personal, financial, and/or business information); internal policies and procedures of EdClub and/or its customers and vendors; product information; personnel information; marketing strategies; financial records or information; trade secrets or any other data that may be considered confidential.

“Data Breach” shall mean an event that causes or could cause the accidental, unauthorized, or unlawful destruction of, loss of, alteration of, disclosure of, or access to, Confidential Information.

“EdClub” or “company” shall mean EdClub, Inc., which includes, individually and collectively, EdClub and its affiliates.

“Employees” shall mean EdClub’s employees, officers, directors, contractors, consultants, temporary workers, and other workers at EdClub.

“Information Systems” shall mean EdClub’s network, accounts, and electronic devices, including Internet/Intranet/Extranet-related systems, computer equipment, mobile devices, licensed and developed software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP servers that EdClub purchases or leases for EdClub’s business purposes or that EdClub permits to access EdClub’s Information Systems, such as Employees’ personal mobile phones to the extent that Employees use such personal devices for EdClub’s business purposes.

“Personal Information” shall mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

“Social Media” shall mean web-based technologies used to broadcast messages and participate in dialogues. Examples of Social Media include social networking applications such as Facebook or MySpace; video-sharing applications such as YouTube; micro-blogging applications such as Twitter; collaboration applications such as Wikipedia; and EdClub’s internal networking tools.

EDCLUB, INC.
DATA BREACH RESPONSE POLICY

1. Overview

This document sets out the processes to be followed in the event that EdClub experiences a Data Breach or suspects that a Data Breach has occurred. It also includes best practices for preventing a Data Breach from recurring, and remedial measures aimed at preventing recurrence once a particular existing Data Breach has been resolved.

This policy mandates that any individual who suspects that a Data Breach has occurred or is about to occur shall contact, and immediately provide a description of the situation to their manager or a member of the Data Breach Response Team. Effective security is a team effort requiring the participation and support of every EdClub employee and affiliate who handles Confidential Information and/or information systems. Every computer user is responsible for knowing these guidelines and reporting potential theft, Data Breaches, or exposures of Confidential Information in accordance with them.

EdClub will investigate all reported Data Breaches and suspected Data Breaches to confirm whether the Data Breach occurred. EdClub shall follow the procedures in this policy if a Data Breach or suspected Data Breach is reported.

2. Purpose

The purpose of the policy is to establish the goals and procedures for responding to a Data Breach. This policy defines what a Data Breach is; roles and responsibilities of staff; and EdClub's reporting, remediation, and feedback mechanisms. The policy shall be well publicized within EdClub and made easily available to all personnel.

Through this policy, EdClub intends to emphasize the importance of data security and detecting and responding to Data Breaches, as well as how EdClub should respond in the context of its established culture of openness, trust, and integrity. EdClub is committed to protecting its customers, employees, partners, and the company itself from illegal or harmful activity by individuals, entities, or state actors, either knowingly or unknowingly.

3. Scope

This policy applies to Employees and covers all Confidential Information and Information Systems.

4. Policy

4.1 Internal Reporting

- 4.1.1 Anyone who becomes aware of an actual or potential Data Breach shall immediately alert EdClub management or a member of the Data Breach Response Team.
- 4.1.2 When reporting an actual or potential Data Breach, the following information shall be provided to the extent it is available:
 - (a) When the actual or potential Data Breach occurred (time and date).
 - (b) Description of the actual or potential Data Breach (type of Confidential Information involved).
 - (c) Cause of the actual or potential Data Breach or how it was discovered.
 - (d) Which systems are affected by the actual or potential Data Breach.
 - (e) Whether corrective action has occurred to remedy or mitigate the actual or potential Data Breach.

4.2 Assessing a Potential Data Breach

- 4.2.1 The criteria for determining whether a Data Breach has occurred include:
 - (a) Is Confidential Information involved? If so, is the Confidential Information of a sensitive nature?
 - (b) Is Personal Information involved?
 - (c) Has there been unauthorized access to Confidential Information or Personal Information? Was Confidential Information or Personal Information not appropriately secured, leaving it accessible to malicious actors?
- 4.2.2 The criteria for determining severity of a Data Breach include:
 - (a) The type and extent of Confidential Information, including Personal Information, involved.
 - (b) Whether multiple individuals have been affected.
 - (c) Whether the information is protected by any security measures (e.g., password protection or encryption).
 - (d) The person or kinds of people who may now have access to Confidential Information, electronic or computing devices, or network resources.
 - (e) Whether there is (or could be) a real risk of serious harm to the affected individuals.

- (f) Whether there could be media or stakeholder attention as a result of the actual or potential Data Breach.

4.3 Data Breach Response Team

4.3.1 EdClub will assemble a team of experts to conduct a comprehensive response in the event of an actual or potential Data Breach.

4.3.2 The EdClub Data Breach response team will include the following individuals:

- (a) The Incident Lead. This person manages the company's response efforts to any actual or potential Data Breach. The Incident Lead may be an internal EdClub employee or an external individual. This is often a legal professional who is experienced in data security matters. Responsibilities of the Incident Lead include acting as an intermediary between senior management and other employees, managing and documenting all response efforts, identifying key tasks, managing the budget and resources needed to handle a Data Breach, and analyzing response efforts to develop forward-looking best practices.
- (b) Company executives. EdClub leaders shall participate in the Data Breach response team to ensure proper leadership, backing, and resources are devoted to the Data Breach response plan.
- (c) IT / security personnel. These individuals will help identify compromised data and train the rest of the Data Breach response team to properly preserve evidence and safely take compromised machines offline.
- (d) Customer care and human resources personnel. These individuals will help to respond to external inquiries about the Data Breach.
- (e) Legal representatives. Internal or external legal data security and compliance experts will help shape any Data Breach response and minimize the risk of litigation and fines. The company's legal representatives should establish relationships with necessary outside counsel before a data breach occurs to ensure necessary support is immediately available during a Data Breach.

4.4 Actions to Take Before a Data Breach Occurs

- (a) Preparedness Training. The Data Breach Response Team shall develop best practices for Data Breach prevention and preparedness for each department at the company. Each member of the Data Breach response team shall work with their department to integrate data security efforts into daily work habits. Employees shall undergo security training at least once per year.
- (b) Regularly update policies. As technology advances and the company updates its systems, data security and mobile device policies shall be reviewed and updated annually or more frequently as necessary to address the adoption of new technology or other material changes in business practices. All changes to data security policies shall be clearly communicated to anyone covered under the scope of this policy.

- (c) Invest in proper cyber security. The company shall periodically engage an independent third party to audit its cyber security software, encryption devices, and firewall protection to make sure these security measures are up to date and effective against potential security threats.
- (d) Contract with vendors ahead of time. The company will establish relationships with forensics experts, data security attorneys, and breach notification experts to make sure these individuals are vetted and available to assist as soon as a Data Breach is suspected or has occurred.

4.5 Responding to a Data Breach

4.5.1 Each incident must be dealt with on a case-by-case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

4.5.2 The Data Breach Response Team has the discretion to make changes to this procedure to adapt to the facts of the Data Breach. The following steps shall be taken in response to a Data Breach:

- (a) Record the date and time when the Data Breach was discovered, as well as the date and time when response efforts begin.
- (b) Alert the Data Breach response team and external resources about the Data Breach and begin executing response procedures.
- (c) Immediately contain the Data Breach. Take all affected equipment offline, but do not turn any machines off until the forensic experts arrive. Closely monitor all entry and exit points, especially those involved in the Data Breach. If possible, put clean machines online in place of affected ones. In addition, update credentials and passwords of authorized users. Secure physical areas potentially related to the Data Breach, including installing locks and changing access codes as needed.
- (d) Evaluate and document the risks associated with the Data Breach, including collecting all available evidence of the Data Breach. Interview people who discovered the Data Breach and all other staff members who have information pertaining to the Data Breach.
- (e) Engage legal counsel with data privacy and security expertise to assess EdClub's potential reporting obligations.
- (f) Create a comprehensive communications plan that reaches all affected audiences — Employees, customers, investors, business partners, and other stakeholders. Do not make misleading statements about the Data Breach or withhold key details that could help individuals protect themselves and their information. Also, do not publicly share information that could put individuals at further risk.
- (g) Develop a media strategy, including the timing, content, and method of any announcements to individuals, regulators, or the media.

4.6 Data Breach Notification

4.6.1 State and federal regulations may require EdClub to notify those who have been affected by the Data Breach, but specific requirements and deadlines for these notifications vary. The General Data Protection Regulation “(GDPR)” may impose additional notification requirements for breaches involving data of individuals who live in the European Union. Therefore, the company shall engage legal counsel to help tailor the notification process to the particular circumstances of the data breach. As required by law, EdClub will provide incident response documents to relevant government regulators upon request, and will reasonably comply with requests from such regulators for follow-up actions reasonably necessary to secure Confidential Information.

4.6.2 The following general guidelines may be used when determining appropriate customer notification procedures:

- (a) Maintain communication with law enforcement. In some jurisdictions, EdClub may delay notification if law enforcement believes it would interfere with an ongoing investigation.
- (b) Multiple state laws may apply to one Data Breach because such laws generally depend on where the affected individuals reside, not where the business is located.
- (c) If some affected individuals live in a jurisdiction that mandates notification and others live in a jurisdiction that does not, the company should notify all affected individuals to avoid the appearance of unequal treatment.
- (d) Consider hiring a professional data breach resolution vendor to handle the notification process, including the administrative requirements associated with printing and mailing notification letters to affected individuals.
- (e) If the breach involved data of individuals who reside in the European Union, ensure all applicable GDPR requirements are met.

4.7 Remedial Measures After a Data Breach

- 4.7.1 Identify lessons learned and remedial action that can be taken to reduce the likelihood of recurrence and implement the necessary administrative, technical, and physical safeguards necessary to prevent recurrence. This may involve a review of policies and training programs.
- 4.7.2 The following steps may be taken to prevent additional Data Breaches from occurring in the future:
- (a) If service providers were involved in the Data Breach, examine whether those service providers have access to Confidential Information and consider changing, limiting, or revoking their access to such data in the future.
 - (b) Consider conducting an audit to reduce the likelihood of such a Data Breach reoccurring in the future.
 - (c) Check network segmentation to make sure the segmentation plan worked as intended.

5. Policy Compliance

5.1 Compliance Measurement

EdClub will verify compliance with this policy through various methods, including but not limited to, business tool reports and internal and external audits.

5.2 Non-Compliance

An Employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Glossary of Terms

Terms that are capitalized but not defined have the meanings assigned to them in applicable EdClub policies or procedures.

“Confidential Information” shall mean important or valuable business information that is not available to the public or personal information. Confidential information includes: Personal Information; customer information (personal, financial, and/or business information); internal policies and procedures of EdClub and/or its customers and vendors; product information; Employee information; marketing strategies; financial records or information; trade secrets or any other data that may be considered confidential.

“Data Breach” shall mean an event that causes or could cause the accidental, unauthorized, or unlawful destruction of, loss of, alteration of, disclosure of, or access to, Confidential Information.

“EdClub” or “company” shall mean EdClub, Inc., which includes, individually and collectively, EdClub and its affiliates.

“Employees” shall mean EdClub’s employees, officers, directors, contractors, consultants, temporary workers, and other workers at EdClub.

“Information Systems” shall mean EdClub’s network, accounts, and electronic devices, including Internet/Intranet/Extranet-related systems, computer equipment, mobile devices, licensed and developed software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP servers that EdClub purchases or leases for EdClub’s business purposes or that EdClub permits to access EdClub’s Information Systems, such as Employees’ personal mobile phones to the extent that Employees use such personal devices for EdClub’s business purposes.

“Personal Information” shall mean information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

“Social Media” shall mean web-based technologies used to broadcast messages and participate in dialogues. Examples of Social Media include social networking applications such as Facebook or MySpace; video-sharing applications such as YouTube; micro-blogging applications such as Twitter; collaboration applications such as Wikipedia; and EdClub’s internal networking tools.

EdClub_Medfield_MA_11State_OHG_fsv response (EdClub 3) CLEAN - EXE (2)

Final Audit Report

2025-09-02

Created:	2025-09-02
By:	TEC SDPA (mmcgrath@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAsIVmeAk1iHO4N16sVP-1fFFs0ynzWp5k

"EdClub_Medfield_MA_11State_OHG_fsv response (EdClub 3) CLEAN - EXE (2)" History

-  Document created by TEC SDPA (mmcgrath@tec-coop.org)
2025-09-02 - 12:21:14 PM GMT
-  Document emailed to EOIN O'CORCORA (eocorcora@email.medfield.net) for signature
2025-09-02 - 12:21:28 PM GMT
-  Email viewed by EOIN O'CORCORA (eocorcora@email.medfield.net)
2025-09-02 - 1:08:14 PM GMT
-  Document e-signed by EOIN O'CORCORA (eocorcora@email.medfield.net)
Signature Date: 2025-09-02 - 1:09:29 PM GMT - Time Source: server
-  Agreement completed.
2025-09-02 - 1:09:29 PM GMT

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: {LEA}, Medfield Public Schools, located at {LEA Address}459 Main Street, Third Floor, Medfield, MA 02052 USA (the “Local Education Agency” or “LEA”) and {Provider}, EdClub, Inc., located at {Provider Address}1701 Pennsylvania Ave. NW, Suite 200, Washington, DC 20006 (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. Only the Supplemental State Terms (if any) for the state of the applicable LEA shall apply.
 - 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.

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.

4.5. 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~~ and/or confidentiality policies for 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~~ applicable law, including 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 within 90 days~~ 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 received from the LEA or any portion thereof as it pertains to the delivery of services to the LEA. Any such audit shall be at no cost to Provider, excluding the Provider employee time, and shall be limited in scope to the LEA's services and data only. 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 of the~~ 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 reasonable 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 aspects of 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's Information Security and Acceptable Use Policy has been provided to LEA prior to signing this DPA. 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 discovered 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 commercially reasonable and 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 and Provider's Terms of Service and Privacy Policy 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~~

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~~would violate Federal, state or local law for the LEA to contract with 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~~will enforce the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, on 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 "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 that has not been de-identified, 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

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.”
4

5. In Article II, Section 4, replace it with the following: “To the extent lawfully permissible: 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).” Current list of subcontractors is attached.
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

~~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”
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 of discovery. The notice shall include: (to the extent available)
 - 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"

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 ~~§§ 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 or assisting with 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 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 of Provider's system, 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.

- (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: (to the extent available):
 - 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 "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and **Medfield Public Schools** ("Originating LEA") which is dated 09/02/2025, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or (3) three years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following **email addresses:**

mohsen@edclub.com & support@edclub.com.

EdClub, Inc

BY: Mohsen Attarpour Date: 8/7/2025

Printed Name: Mohsen Attarpour Title/Position: Authorized Person

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the **Medfield Public Schools** and the Provider.

****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

By: **Andrea Galenski**

Date: 2025-09-23

Printed Name: Andrea Galenski

Title: Superintendent of Schools

SCHOOL DISTRICT NAME: Cheektowaga-Sloan Union Free School District

DESIGNATED REPRESENTATIVE OF LEA:

Name: Brian Zybala

Title: Director of Data and Techonlogy

Address: 166 Halstead Ave, Sloan, NY 14212

Phone: 716-897-7888

Email: bzybala@cheektowagasloan.org

District Policy URL: https://sdpc.a4l.org/ny_dp_bor_url.php?districtID=13038

Bill of Rights URL: https://sdpc.a4l.org/ny_dp_bor_url.php?districtID=13038