



# Standard Student Data Privacy Agreement

Illinois Mathematics and Science Academy (IMSA)

and

Council for Aid to Education (CAE)

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:

Illinois Mathematics and Science Academy, located at 1500 Sullivan Rd, Aurora, IL 60506 [‘Agency’],

AND

[ Council for Aid to Education, Inc. ], located at [ 1732 1st Ave; New York, NY 10128 ] [‘Provider’].

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

**WHEREAS**, the Provider and Agency 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 Agency 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, Agency and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by Agency to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. Special Provisions. Check if Required:  
 If checked, Agency and Provider agree to the additional terms or modifications set forth in Exhibit “F”. (Optional)
3. In the event of a conflict between the Standard Clauses, the 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 be effective upon the date of signature by Provider and Agency, and shall remain in effect as between Provider and Agency 1) for so long as the Services are being provided to the Agency or 2) until the DPA is terminated pursuant to Article VI, Section 1, whichever comes first.
5. The services to be provided by Provider to Agency pursuant to this DPA are detailed in Exhibit “A” (the “Services”).
6. Notices. Pursuant to SOPPA, the Agency shall publish on its website a copy of the fully executed DPA between the Provider and Agency with signatures redacted. 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 DPA representative for the Agency is:

Name: Richard Busby            Title: Interim Privacy Officer

Address: 1500 Sullivan Road, Aurora, IL 60506    Phone: (630) 907-5022

Email: rbusby@imsa.edu

The designated DPA representative for the Provider is:

Name: Rene Smith

Title: CTO

Address: 1732 1st Ave; New York, NY 10128

Phone: +1 212.217.0864

Email: rsmith@cae.org

IN WITNESS WHEREOF, Agency and Provider execute this Agreement as of the Effective Date.

Agency:

By: Click or tap here to enter text.

Date: Click or tap to enter a date.

Printed Name:

Title/Position:

Provider:

By: Click or tap here to enter text.

Date: July 7, 2022

Printed Name: Bob Yayac

Title/Position: CEO & President

## **STANDARD CLAUSES**

Version 1.0

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

**1. Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, and pursuant to the federal Family Educational Rights and Privacy Act of 1974, the Provider shall be considered a School Official with a legitimate educational interest, is performing an institutional service or function for which the Agency would otherwise use its own employees; is under the direct control and supervision of the Agency 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.

**2. Student Data to Be Provided.** In order to perform the Services described above, Agency shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

**3. DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

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

**1. Student Data Property of Agency.** 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 Agency. 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 Agency. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the Agency as it pertains to the use of Student Data, notwithstanding the above.

**2. Parent Access.** To the extent required by law the Agency 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 ten (10) days from the date of the request or pursuant to the time frame required under state law for an Agency to respond to a parent or student, whichever is sooner) to the Agency'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 Agency, who will follow the necessary and proper procedures regarding the requested information.

**3. Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the Agency, transfer, or provide a mechanism for the Agency to transfer, said Student-Generated Content to a separate account created by the student.

**4. Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the Agency in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the Agency of the request.

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

### ARTICLE III: DUTIES OF AGENCY

**1. Provide Data in Compliance with Applicable Laws.** Agency shall provide Student Data, which may include all or a portion of that listed in Exhibit 'B' 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 Agency has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), Agency 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.** Agency 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.** Agency shall notify Provider promptly of any known unauthorized access. Agency 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, as all may be amended from time to time.

**2. Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit A** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

**3. Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

**4. No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the Agency 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 subcontractors performing services on behalf of the Provider pursuant to this DPA. Provider will not sell Student Data to any third party.

**5. De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the Agency 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 Agency learning purpose and for customized student Agency learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by Agency to return or destroy Student Data. Except for Subcontractors, 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 Agency who has provided prior written consent for such transfer. Prior to publishing any document that names the Agency explicitly or indirectly, the Provider shall obtain the Agency's written approval of the manner in which de-identified data is presented.

**6. Disposition of Data.** Upon written request from the Agency, Provider shall dispose of or provide a mechanism for the Agency 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 Agency is received, Provider shall dispose of all Student Data after providing the Agency with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The Agency may utilize a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the Agency 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 Agency . This section does not prohibit Provider from using Student Data (i) for adaptive Agency learning or customized student Agency learning (including generating personalized Agency learning recommendations); or (ii) to make product recommendations to teachers or Agency 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

## **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 Agency, 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 Agency with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the Agency to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the Agency. The Provider will cooperate reasonably with the Agency 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 Agency, and shall provide reasonable access to the Provider's facilities, staff, agents and Agency's Student Data and all records pertaining to the Provider, Agency and delivery of Services to the Agency. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

**3. Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The Provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "E"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "F"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "E"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who Agency 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 Agency within seventy-two (72) hours of confirmation of the incident, but no later than thirty (30) days after determination that a breach occurred, 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:
  - a. The name and contact information of the reporting Agency subject to this section.
  - b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
  - c. 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.

- d. 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
  - e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
  - f. A list of students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and
  - g. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.
- (2) In the event of a Data Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the Agency for any and all costs and expenses that the Agency incurs in investigating and remediating the Breach, without regard to any limitation of liability provision otherwise agreed to between the Provider and Agency, 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 to 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 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 school 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 of any other State or federal laws.
- (3) 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.
- (4) 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 Agency , upon request, with a summary of said written incident response plan.
- (5) Agency shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (6) In the event of a breach originating from Agency's use of the Service, Provider shall cooperate with Agency to the extent necessary to expediently secure Student Data.

**5. Transfer or Deletion of Student Data.** The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to this agreement 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 this Agreement and this DPA, the Provider will provide written notice to the Agency as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to Agency, as directed by the Agency, within 30 calendar days if the Agency requests deletion or transfer of the Student Data and shall provide written confirmation to the Agency of such deletion or transfer. Upon termination of the Service Agreement between the Provider and Agency, the Provider shall conduct a final review of Student Data within 60 calendar days.

If Agency received a request from a parent, that Student Data being held by the Provider be deleted, the Agency shall determine whether the requested deletion would violate State and/or federal records laws. If the determination is no violation is applicable, the Agency 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.

6. **Subcontractors.** Provider, no later than (5) business days after the date of execution of this Agreement, must provide to Agency a list, or a link to a page on the Provider's website, of any subcontractors, third parties or affiliates to whom the Provider or Operator is currently disclosing covered information or has disclosed covered information. This list must, at a minimum, be updated and provided to the Agency at the beginning of each State fiscal year (July 1) and at the beginning of each calendar year (January 1).

## **ARTICLE VI: 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 upon a material breach by the other party.

**2. Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of Agency'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.

**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 Illinois, without regard to conflicts of law principles. Each party consents and submits to the sole and exclusive jurisdiction to the State and Federal courts of Kane County 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 Agency 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 Agency has the authority



to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging or otherwise disposing of its business.

**8. Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

**9. Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

**EXHIBIT 'A' – DESCRIPTION OF SERVICES**

The Council for Aid to Education, Inc (“CAE”) provides assessments that measure of critical thinking, problem solving and written communication skills for students.

**EXHIBIT 'B' – DATA COLLECTION**

(Check box for each item collected and used by your system)

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Name (First)   | <input type="checkbox"/> Health Records  |
| <input checked="" type="checkbox"/> Name (Last)  | <input type="checkbox"/> Medical Records   |
| <input type="checkbox"/> Home Address  | <input type="checkbox"/> Social Security Number                                    |
| <input type="checkbox"/> Telephone Number  | <input type="checkbox"/> Biometric Information (ie: fingerprints, facial patterns) |
| <input type="checkbox"/> Cell Phone Number   | <input type="checkbox"/> Disabilities  |
| <input type="checkbox"/> Photos  | <input type="checkbox"/> Date of Birth   |
| <input type="checkbox"/> Disciplinary Records  | <input type="checkbox"/> Food Purchases  |
| <input checked="" type="checkbox"/> Test Results   | <input type="checkbox"/> Political Affiliations                                    |
| <input type="checkbox"/> Special Education Data  | <input type="checkbox"/> Religious Information                                     |
| <input type="checkbox"/> Juvenile Dependency Records   | <input type="checkbox"/> Text Messages   |
| <input type="checkbox"/> Grades  | <input type="checkbox"/> Student Identifiers                                       |
| <input checked="" type="checkbox"/> Evaluations  | <input type="checkbox"/> Search Activity   |
| <input type="checkbox"/> Criminal Records  | <input type="checkbox"/> Voice Recordings  |
| <input checked="" type="checkbox"/> Socioeconomic Information  | <input type="checkbox"/> Geolocation Information                                   |
| <input checked="" type="checkbox"/> Email Address or other information that allows physical or online contact. | <input type="checkbox"/> Other (Please describe) _____                             |

### **EXHIBIT "C" - DEFINITIONS**

**Breach:** The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of covered information maintained by an operator or school. "Covered information" means personally identifiable information or material or information that is linked to personally identifiable information or material in any media or format that is not publicly available and is any of the following:

- (1) Created by or provided to an operator by a student or the student's parent in the course of the student's or parent's use of the operator's site, service, or application for school purposes.
- (2) Created by or provided to an operator by an employee or agent of a school for school purposes.
- (3) Gathered by an operator through the operation of its site, service, or application for school purposes and personally identifies a student, including, but not limited to Student Data(as defined herein)

**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 by a person acting for such school, 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 primarily 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 the Agency to provide a service to that Agency shall be considered an "operator" for the purposes of this section.

**Parent:** The meaning given to that term as defined under the Illinois School Student Records Act 105 ILCS 10/2(g).

**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.

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

**Student Data:** Student Data includes any data, whether gathered by Provider, Operator or provided by Agency or its users, students, or students' parents/guardians, that personally identifies a 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 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.

**Subcontractor:** A party other than Agency 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.

**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 request for information or feedback.

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

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

Provider is to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between Agency and Provider. The terms of the Disposition are set forth below:

##### **1. Extent of Disposition**

- Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:
  
- Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

- Disposition shall be by destruction or deletion of data.
- Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

Click or tap here to enter text.

3. Schedule of Disposition

Data shall be disposed of by the following date:

- As soon as commercially practicable.
- By  Click or tap to enter a date.

4. Signature

\_\_\_\_\_  
Authorized Representative of Agency

Click or tap to enter a date.

Date

5. Verification of Disposition of Data

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

Click or tap to enter a date.

Date

**EXHIBIT "E" - DATA SECURITY REQUIREMENTS**

**Adequate Cybersecurity Frameworks**

**2/24/2022**

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles\* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks: (Check all applicable boxes that are utilized by the Provider.)

	<b>MAINTAINING ORGANIZATION/GROUP</b>	<b>FRAMEWORK(S)</b>
<input type="checkbox"/>	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
<input 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)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

\*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here.

**EXHIBIT "F" – Additional Terms or Modifications**

**(IMSA Legal Review required for any items listed in Exhibit F)**

Agency and Provider agree to the following additional terms and modifications:

If there are None, type 'None' in the box.

