Standard Student Data Privacy Agreement

Illinois Mathematics and Science Academy (IMSA)

and

[ ]

Council for Aid to Education, Inc. 1732 1st Ave; New York, NY 10128

Rene Smith CTO

1732 1st Ave; New York, NY 10128 +1 212.217.0864

rsmith@cae.org

July 7, 2022

Bob Yayac CEO & President

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)

☒	Name (First)	☐	Health Records
☒	Name (Last)	☐	Medical Records
☐	Home Address	☐	Social Security Number
☐	Telephone Number	☐	Biometric Information (ie: fingerprints, facial patterns)
☐	Cell Phone Number	☐	Disabilities
☐	Photos	☐	Date of Birth
☐	Disciplinary Records	☐	Food Purchases
☒	Test Results	☐	Political Affiliations
☐	Special Education Data	☐	Religious Information
☐	Juvenile Dependency Records	☐	Text Messages
☐	Grades	☐	Student Identifiers
☒	Evaluations	☐	Search Activity
☐	Criminal Records	☐	Voice Recordings
☒	Socioeconomic Information	☐	Geolocation Information
☒	Email Address or other information that allows physical or online contact.	☐	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.)

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

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.