

Data Processing Agreement

The terms of this Data Processing Agreement (“**DPA**”) are referenced in the Master Services Agreement (“**MSA**”) and hereby incorporated into the Agreement entered into by the “**Institution**” and Innovative Educational Solutions, Inc. d/b/a Entrypoint (“**Entrypoint**”) (individually a “**Party**”, together the “**Parties**”) in conjunction with the licensing of the EntryPointSRM software (the “**Software**”) to the Institution. This DPA is effective as of the signature date on the most recent Order Form between the Parties (the “**Effective Date**”). In the event of a conflict between this DPA or any other writing between the Parties, this DPA shall control with respect to the subject matter herein.

The Parties agree as follows:

1. Definitions.

- “**Affiliate(s)**” means any entity, subsidiary, parent, or other organization that shares at least 50% ownership with a party.
- “**Institution Data**” means any proprietary or confidential data provided by Institution to Entrypoint or created by Entrypoint on behalf of Institution in the provision of the Services. Institution Data includes without limitation Educational Records and Personally Identifiable Information (as defined below) and includes confidential information as defined in the Master Services Agreement and Terms and Conditions. Institution Data does not include data used by the Entrypoint for internal operations.
- “**Data Breach**” means an actual breach, or reasonable suspicion, of a breach of security, privacy, or Data Protection Laws leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Institution Data created, transmitted, stored, or otherwise Processed by Entrypoint.
- “**Data Protection Law(s)**” means the laws and regulations that are applicable to the Processing of Personally Identifiable Information or Institution Data Processed by Entrypoint under this DPA, including without limitation, FERPA (defined below), the Children’s Online Privacy and Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6505 and 16 CFR Part 213, the Protection of Pupil Rights Amendment at 34 CFR Part 90 (“**PPRA**”), the Children’s Internet Protection Act at 20 U.S.C. § 9132 and 254 (“**CIPA**”) and any applicable U.S. federal and state laws governing the protection of Personally Identifiable Information.
- “**De-identified Data**” means data and information where all Personally Identifiable Information has been removed or obscured such that the remaining data and 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 individual. Provided, however, data sets with less than twenty (20) individuals are not considered “de-identified”.

- **“Disclosure”** means to permit access to or the release, transfer or other communication of Personally Identifiable Information or Education Record by any means, including oral, written, or electronic means, to any unauthorized third-party.
- **“Educational Records”** means records, files, documents, and other materials directly related to a student including Student Generated Content and created or maintained by the Institution, or by a person acting on behalf of the Institution.
- **“FERPA”** means the Family Educational Rights and Privacy Act at 20 U.S.C. § 1232g and regulations at 34 CFR Part 99.
- **“Personally Identifiable Information”** or **“PII”** means any information relating to an identified or reasonably identifiable individual. This includes indirect information or identifiers; or other information that, alone or in combination, is linked or linkable to a specific person that would allow a reasonable person, who does not have personal knowledge of the relevant circumstances, to identify an individual with reasonable certainty.
- **“Processing”** means any operation or set of operations which is performed upon Personally Identifiable Information whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, Disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction (**“Process”**, **“Processes”** and **“Processed”** shall have the same meaning).
- **“School Official”** means an entity that, (a) performs an institutional service or function for which the Institution would otherwise use employees; (b) is under the direct control of the Institution with respect to the use and maintenance of Student Data including Education Records; and (c) Is subject to 34 CFR § 99.33(a) governing the use and re-Disclosure of Personally Identifiable Information from Education Records.
- **“Service Agreement”** means the current contract for Services between the Institution and Entrypoint consisting of the Master Services Agreement, incorporated Terms and Conditions, the Order Form and this DPA.
- **“Services”** means the software, services, or other materials described in the Service

Agreement and includes the underlying infrastructure, hosting, and networks.

- **“Student Generated-Content”** means any content created by a student through their direct use of the Services, including, but not limited to, notes, transcriptions, audio files, and images, except "student-generated content" does not include data about a student not directly entered into the Software by a student themselves.
- **“Subprocessor(s)”** means any third-party engaged by the Entrypoint that Processes Personally Identifiable Information or Education Records on behalf of the Entrypoint.

2. Term; Termination.

2.1 Term.

This DPA is effective for the duration of the MSA.

2.2 Termination.

During the term of the Service Agreement, this DPA may only be terminated in accordance with the terms of the MSA. In the event of such termination, Entrypoint shall stop Processing Institution Data and dispose of Institution Data as described in Section 4.9.

This DPA shall automatically terminate upon the same date as the Service Agreement unless otherwise agreed to by the Parties. In the event of such termination, Entrypoint shall stop Processing Institution Data and dispose of Institution Data as described in Section 4.9.

3. Data Use, Ownership, and Obligations.

3.1 **Data Ownership.** Institution retains all ownership and control of Institution Data, including any modifications or copies. All Institution Data remains the Institution's exclusive property and is subject to this DPA.

3.2 **Data Location.** Entrypoint will store or host all Educational Records and Personally Identifiable Information in the continental USA.

3.3 **FERPA.** To the extent that the Institution is subject to FERPA, the Parties agree that Entrypoint operates as a School Official under FERPA and has a legitimate educational interest in Personally Identifiable Information from Education Records received from the Institution pursuant to this DPA. For purposes of the Agreement and this DPA, Entrypoint: (a) provides a service or function for which the Institution would otherwise use its' employees; (b) is under the direct control of the Institution with respect to the use and maintenance of Education Records; and (c) is subject to the requirements of FERPA governing the use and re-Disclosure of

Personally Identifiable Information from the Education Records received from Institution.

3.4 **Separate Account.** While no Student Generated Content is expected to be created, stored or maintained by Entrypoint, as required and defined by applicable Data Protection Laws, if Student Generated Content is created, stored, or maintained by Entrypoint or the Services, Entrypoint shall, at the request of the Institution, transfer or provide a mechanism for the Institution to transfer such Student Generated Content to a separate account created by the student or parent.

3.5 **De-Identified Data.** De-Identified data may be used by Entrypoint for those purposes permitted under FERPA and the following purposes: (a) assisting the Institution or other governmental agencies in conducting research and other studies; (b) research and development of Entrypoint's educational sites, software, services, business processes or other applications, (c) to demonstrate the effectiveness of the Services; and (d) aggregated by Entrypoint for performing analytics and trends across similarly-situated Institutions. Entrypoint's use of De-Identified Data shall survive termination of this DPA or any request by Institution to return or destroy Student Data. Entrypoint agrees not to attempt to re-identify De-Identified Data, and not to transfer De-Identified Student Data to any third party unless that third party agrees in writing not to attempt re-identification.

4. Entrypoint Obligations.

4.1 **Authorized Use.** Entrypoint shall only use Institution Data as provided in this DPA and the Service Agreement to provide the Services. Except as expressly permitted herein, Entrypoint shall not disclose Institution Data to any third party without the prior written consent of Institution. Entrypoint may only share Institution Data with its Affiliates to provide the Services under the Agreement and any such access shall be on a need-to-know basis.

4.2 **Compliance with Data Protection Laws.** In its provision of the Services, Entrypoint agrees to comply with all Data Protection Laws applicable to its Processing of Institution Data.

4.3 **Advertising.** Entrypoint shall not sell, transfer, share, or otherwise disclose Personally Identifiable Information, Education Records, unique identifiers, or any Institution Data to targeted advertising providers or develop a profile of a student or parent or guardian for the purpose of advertising. Entrypoint will not use Personally Identifiable Information for its own advertising or for third-party advertising. This does not prohibit Entrypoint from using Institution Data to provide adaptive counseling services, customized student learning services, making product recommendations to Institution employees, and notify account holders of updates about the Services or new features of the Services.

4.4 Entrypoint Personnel. Entrypoint shall ensure that its employees, Subprocessors, subcontractors, and agents (collectively “Personnel”) involved in the Processing of Personally Identifiable Information or Education Records are subject to either contractual or statutory obligations of confidentiality, and that access is strictly limited to those Personnel who require access to perform the Services. Entrypoint shall ensure that its Personnel are informed of the confidential nature of the Institution Data and have received appropriate training on their responsibilities and applicable Data Protection Laws. As required by Data Protection Laws or Institution policy, Entrypoint shall ensure that its Personnel have gone through appropriate background checks prior to accessing Personally Identifiable Information or Education Records.

4.5 Security and Privacy.

(a) Security and Privacy Program. Entrypoint shall implement and maintain a security and privacy program that includes appropriate physical, administrative, technical, and operational controls to protect the confidentiality, integrity, privacy, and availability of Institution Data Processed by Entrypoint aligned with an industry standard framework such as the NIST Cybersecurity Framework, AICPA SOC 2 Type 2, ISO/IEC 27001, or other recognized industry standards. These measures shall include protection against unauthorized or unlawful access, processing, loss, alteration, damage of Institution’s Personally Identifiable Information. Entrypoint shall regularly monitor its compliance with its program and not materially decrease its privacy and security controls during the term of this DPA.

(b) Incident Response Plan. Entrypoint shall implement, maintain, and regularly test an incident response plan consistent with industry standard practices and Data Protection Laws. This incident response plan shall include processes for responding to a Data Breach, breach of the security, privacy, or unauthorized acquisition or use of Institution Data or any portion thereof, including PII and agrees to provide Institution with a summary of said written incident response plan so long as a valid non-disclosure agreement in place between the parties.

4.6 Data Breach. In the event of a Data Breach, Entrypoint shall promptly, but in no more than seventy-two (72) hours, notify Institution of any such Data Breach unless prohibited by an applicable law enforcement authority. Entrypoint shall provide such notification to Institution’s Security Contact as described in Section 7.5 or other contact as provided by Institution. In such notification Entrypoint shall provide the following information, to the extent such information becomes available to Entrypoint; (a) a general description of the Data Breach; (b) the categories and approximate number of records or individuals affected by the Data Breach; (c) actions taken by Entrypoint to remediate the Data Breach; and (d) Entrypoint shall (i) take reasonable steps to mitigate the effects and minimize any damage resulting from the Data Breach; (ii) cooperate

with Institution's reasonable requests for assistance in remediating a Data Breach; and (iii) maintain records of information related to the Data Breach. If such information is not available within the timeframe specified, the Entrypoint shall include an estimated timeline to provide a complete detail of the above aspects.

4.7 Audits. No more than once every twelve (12) months, Institution may conduct an audit of Entrypoint's compliance with this DPA and applicable Data Protection Laws for the purpose of meeting its obligations under Data Protection Laws or Institution's policies. Such audit shall be limited to the review of documentation, questionnaires, and related non-intrusive methods. Institution shall provide at least thirty (30) days written notice to Entrypoint of such an audit. Under no circumstances shall the audit include penetration tests, code reviews, or any other actions that could be disruptive to the Software in production or potentially violate the confidentiality or expose the intellectual property of the Entrypoint.

(a) In lieu of an Institution audit, Entrypoint may conduct a third-party security and privacy audit of its Services and program. Upon receipt of a written request and execution of an appropriate confidentiality agreement, Entrypoint will provide copies of its most recent audit summary or bridge letter to Institution.

(b) In the event of a Data Breach, or inquiry by any governmental agency, Institution (or the applicable governmental agency) may perform an audit of Entrypoint upon written notice to Entrypoint. Institution shall send any such audit request to the Security Contact identified in Section 7.5 (Notice). In the event that Institution engages a third party to perform the audit, such third party shall execute a non-disclosure agreement with Entrypoint. Institution agrees to promptly notify the Entrypoint of any non-compliance discovered during such an audit.

(c) Entrypoint agrees in good faith to remediate any critical or high security findings, or known exploitable findings identified by the Institution.

4.8 Subprocessors. Institution agrees that Entrypoint may use Subprocessors in connection with the provision of the Services and permit Subprocessors to Process Institution Data, provided that:

(a) Entrypoint shall ensure that obligations not materially less protective than those set out in this DPA, and applicable Data Protection Laws are imposed on its Subprocessors;

(b) Entrypoint shall be responsible for the acts and omissions of its Subprocessors if and to the same extent Entrypoint would be liable if performing the services of each Subprocessor directly;

(c) Entrypoint shall provide Institution of a list of its current Subprocessors in Exhibit A or

by providing a link to a website where information about its list of Subprocessors are kept up to date; and

(d) Entrypoint shall inform the Institution of any changes or additions to its Subprocessors at least thirty (30) days prior to such addition or change.

4.9 Deletion and Return of Institution Data.

(a) Entrypoint shall (and ensure that its Subprocessors shall) securely delete Institution Data stored in the Services (i) within ninety (90) days after termination of this DPA; or (ii) within thirty (30) days upon written request from Institution. Upon written request from Institution, Entrypoint shall provide written certification of such deletion substantially in the form of Exhibit B. Until such deletion occurs, the Entrypoint will ensure compliance with this DPA.

(b) Entrypoint shall provide functionality for the Institution to download Institution Data from the Services, to the extent possible provided by the Services. If the Services do not provide a download functionality, the Entrypoint shall return to Institution all Institution Data in the Services in an industry standard format within ninety (90) days after termination of this DPA.

(c) If Entrypoint believes that it cannot comply with the foregoing deletion requirement because applicable law requires the retention of such data then Entrypoint shall provide written notice to Institution within thirty (30) days of termination of this DPA informing of such requirement and protect such data in accordance with this DPA.

4.10 Law Enforcement Requests. If Entrypoint receives a request for access to Institution Data from a legally authorized entity, the Entrypoint shall promptly notify Institution of such request unless prohibited from such notification by applicable law.

5. Institution Obligations.

5.1 Institution shall, in its use or receipt of the Services, Process Institution Data in accordance with the Data Protection Laws. Institution will ensure that its instructions for the Processing comply with applicable Data Protection Laws. Institution shall have sole responsibility for the accuracy, quality, and legality of Institution Data, the means by which Institution obtained the Institution Data, and for fulfilling all requirements under Data Protection Laws necessary to make the Institution Data available to Entrypoint. Institution shall promptly notify Entrypoint of any known unauthorized access to the Services. Institution will assist Entrypoint in any efforts by Entrypoint to investigate and respond to any unauthorized access to the Services.

5.2 COPPA Obligations. Personally Identifiable Information about children under 13 may

only be used by the Services with prior consent of a parent or an educational institution acting on behalf of the child's parent. Institution agrees that it has obtained such consent prior to storing or processing any Personally Identifiable Information of any child under 13 in the Software

6. Insurance.

In addition to any insurance requirements under the Service Agreement, Entrypoint shall secure and maintain at Entrypoint's sole expense the insurance coverages described Exhibit C.

7. Miscellaneous

7.1 Severance. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, construed in a manner as if the invalid or unenforceable part had never been contained therein.

7.2 Entire Agreement. This DPA and the Service Agreement constitutes the entire agreement of the Parties with respect to the subject matter hereof and supersedes any prior or contemporaneous representations, understandings, writings, or agreements by the Parties. This DPA may only be amended by the Parties in writing.

7.3 Governing Law; Jurisdiction; Venue. This DPA shall be governed by and construed in accordance with the laws of the state of Indiana without regard to conflicts of laws principles. The Parties agree to submit to the jurisdiction of the state and federal courts located in Indiana.

7.4 Assignment. Entrypoint may not assign its rights and obligations under this DPA without the consent of the Institution which shall not be unreasonably withheld. Any such assignment without consent shall be considered null and void. Notwithstanding the foregoing, Entrypoint may assign its rights and obligations under this DPA, in whole or part, in connection with the transfer or sale of all or substantially all of the assets or business of Entrypoint. This DPA will be binding upon, inure to the benefit of, and be enforceable by the Parties and respective successors and permitted assigns.

7.5 Notices. Any notice required or permitted to be given under this DPA shall be in writing and shall be addressed to the appropriate Party at the address specified in the MSA. Notices shall be deemed to have been given for all purposes (a) when delivered if sent by a reputable courier service, or (b) five (5) days after mailing, or (c) upon receipt when delivered by email provided that the recipient acknowledges such delivery.

7.6 This Data Processing Agreement is effective upon signing of the MSA and is

incorporated into the MSA between Parties.

Exhibit A - Subprocessor List

Entrypoint's currently approved Subprocessors are listed below.

Subprocessor Name	Subprocessor Address	Processing Activities	Institutional Data Processed	Processing or Hosting Location
Google Cloud	Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	Hosting, Storage	None- hosts application but no direct access to Institutional Data	United States
OpenAI	OpenAI OpCo, LLC 1455 3rd Street San Francisco, CA 94158 USA	Converts natural language queries to data queries	Any institutional data queried in the database	United States
SupaBase	Supabase, Inc. 548 Market St San Francisco, CA 94104 USA	Hosting, Storage	Hosts data in encrypted form, no direct access to Institutional Data	United States

Exhibit B - Data Deletion Certificate Template

The undersigned hereby certifies that all copies of Institution Data collected, created, or processed by Entrypoint on behalf of _____ (“Institution”) have been securely deleted from Entrypoint’s Services on _____.

By signing, Entrypoint confirms all Institution Data in any form has been properly disposed of according to the Data Privacy and Security Agreement. This includes all copies, derivatives, backups, and temporary files held by Entrypoint and its subcontractors.

Signature

Name

Title

EXHIBIT C
Risk Insurance Policy

Chubb DigiTech® Enterprise Risk Management Policy

Account: Innovative Educational Solutions Inc.

Agent: CHITTICK ADVISORY GROUP INC

Producer Code: Z11001

Writing Company: ACE American Insurance Company

Effective Date: 11/01/2025 – 11/01/2026