Data Processing Addendum

1. Scope

1.1 This Data Processing Addendum ("**DPA**") by and between Scenario Learning, LLC d/b/a Vector Solutions ("Service Provider") and the undersigned Client (each a "Party" and collectively the "Parties"), is effectively incorporated into the Vector Solutions Education Software as a Service Agreement concurrently entered into between Service Provider and Client ("**Agreement**").

1.2 This DPA is effective as of the date of the Agreement. In the event of a conflict between any provisions of, or attachments to, the Agreement and the provisions of this DPA, the provisions of this DPA shall govern and control.

1.3 From time to time, the Parties may amend this DPA to clarify the understanding of the relationship of the Parties with respect to Data Protection Laws, as herein defined, effective after the effective date of this DPA, and to clarify the obligations of each Party thereunder.

2. Definitions

2.1 "**Personal Information**" means information about an individual that (i) can be used to identify, contact, or locate a specific individual; (ii) can be combined with other information that is linked to a specific individual to identify, contact, or locate a specific individual; and/or (iii) is defined as "personal data" or "personal information" by applicable Data Protection Law.

2.2 "**Security Incident**" means (i) any act or omission that compromises either the security, confidentiality, or integrity of Personal Information or the physical, technical, administrative, or organizational safeguards put in place by Service Provider that relate to the protection of the security, confidentiality, or integrity of Personal Information, or (ii) receipt of a complaint in relation to the privacy and data security practices of Service Provider or a breach or alleged breach of this DPA. Without limiting the foregoing, a compromise shall include any unauthorized access to, disclosure of, or acquisition of Personal Information.

2.3 "**Data Protection Laws**" means all applicable laws, regulations, and requirements of regulatory guidance, in any jurisdiction anywhere in the world, relating to data protection, privacy, and confidentiality of Personal Data—including, where applicable, the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR"), and the California Consumer Privacy Act, sections 1798.100 to 1798.199, Cal. Civ. Code (2018) ("CCPA")—and any implementing, derivative or related legislation, rule, regulation, and regulatory guidance, as amended, extended and re-enacted from time to time.

2.4 "**Data Subject**" means an identified or identifiable natural person to whom Personal information relates.

2.5 "**Processing**" means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Any capitalized terms not otherwise defined in this DPA shall have the meaning given to them in the Agreement.

3. Obligations

3.1 Client shall determine the scope, purposes, and manner by which the Personal Information in Schedule 1 may be accessed or Processed by Service Provider.

3.2 Client is responsible for compliance with its obligations as a data controller (or the equivalent) under Data Protection Laws, in particular for justification of any transmission of Personal Information to Service Provider (including providing any required notices of the engagement of Service Provider for Processing, and obtaining any required consents and/or authorizations, or otherwise securing an appropriate legal basis under Data Protection Laws, where applicable), and for its decisions and actions concerning the Processing of such Personal Information.

3.3 Service Provider is responsible for compliance with its obligations as a data processor (or the equivalent) under Data Protection Laws. Service Provider and any persons acting under its authority including any of its employees, agents, contractors and/or subprocessors shall Process the Personal Information only as set forth in Client's written instructions as specified in the Agreement and this DPA to the extent such Processing is required for the provision of Service Provider's services.

3.4 Without prejudice to any existing contractual arrangements between the Parties, Service Provider shall treat all Personal Information as confidential and shall inform all its employees, agents, contractors and/or subprocessors engaged in Processing Personal Information of the confidential nature of the Personal Information consistent with the confidentiality provisions set forth in the Agreement. Service Provider shall ensure that all such persons or parties are bound to a duty of confidentiality or are under an appropriate statutory obligation of confidentiality.

3.5 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Service Provider shall implement reasonable and appropriate technical and organizational measures designed to protect the Personal Information against unauthorized or unlawful Processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, destruction, or damage. Service Provider's or its subprocessors' adherence to either an approved code of conduct or to an approved certification mechanism recognized under Data Protection Law may be used to satisfy the requirements of this Section.

3.6 Service Provider shall not sell (for monetary consideration), retain, use, or otherwise disclose Personal Information for any purpose other than for performing the services described in the Agreement in accordance with the Client's written instructions, or as otherwise permitted by law.

3.7 Service Provider shall reasonably assist Client by appropriate technical and organizational measures for the fulfillment of Client's obligation to respond to requests for exercising the Data Subject's rights under Data Protection Laws.

3.8 Service Provider shall notify Client without undue delay of becoming aware of any Security Incident, as defined above. Service Provider shall use reasonably commercial efforts to provide Client with sufficient information to allow it to meet any obligations to inform regulators and/or Data Subjects of the Security Incident, and to perform an investigation into the Security Incident. The obligations herein shall not apply to Security Incidents caused by Client.

3.9 If Service Provider receives any subpoena, judicial, administrative, or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority which relates to the Processing of Personal Information ("Disclosure Request"), it shall promptly pass on such Disclosure Request to Client without responding to it, unless otherwise required by applicable law (including to provide an acknowledgement of receipt to the authority that made the Disclosure Request).

3.10 Where required, the Parties agree to negotiate in good faith and enter into any further data processing or transfer agreement, including any standard contractual clauses for transfers of data outside of the country where the personal data originates, as may be required to comply with Data Protection Laws.

3.11 It is the Parties' good faith belief that Service Provider's services under the Agreement do not implicate any applicable cybersecurity or national security laws of any country. In an abundance of caution,

Client shall be responsible for any cybersecurity or national security obligations arising out of its use of Service Provider's services outside of the United States, including any data localization requirements or security assessments of a foreign jurisdiction. Service Provider shall exercise good faith in cooperating with Client in demonstrating such compliance, if needed.

4. Indemnification and Limitation of Liability

4.1 The indemnification and limitation of liability provisions in the Agreement are incorporated herein by reference and made a part of this DPA and shall apply to any claim arising out of a breach of this DPA.

4.2 Notwithstanding the forgoing, each Party acknowledges that its breach of this DPA may cause irreparable damage to the other Party and hereby agrees that the other Party will be entitled to seek injunctive relief under this DPA, as well as such further relief as may be granted by a court of competent jurisdiction.

5. Duration and Termination

5.1 The termination or expiration of this DPA shall not discharge Service Provider from its confidentiality obligations pursuant to the Agreement and this DPA. Service Provider shall Process Personal Information until the date of expiration or termination of the Agreement, unless instructed otherwise by Client, or until such data is returned, de-identified, or destroyed on instruction of Client.

5.2 Upon termination or expiration of this DPA or at any time at Client's written request, Service Provider shall return to Client, or destroy, all Personal Information, except as otherwise permitted by Data Protection Law or other applicable laws or regulations.

6. Miscellaneous

6.1 Any disputes arising from or in connection with this DPA shall be brought as set forth in the Agreement.

6.2 Notice by one Party to the other Party shall be made as set forth in the Agreement.

6.3 This DPA may be executed in two or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to constitute one and the same document. The parties deliver this DPA by facsimile or email transmission.

In consideration of the mutual promises herein, the parties have executed this DPA as of the date set forth below.

Vector Solutions	Client
By: Justin Moore	By: RJ DeLisle
Name: Justin Moore	Name: RJ DeLisle
Title: K12 Sales Director	Title: DATA PRIVACY OFFICER
Date: 6/22/21	Date: 1-31-2023

Exhibit 1

Subject Matter and Nature of Processing,
Categories of Personal Information,
Categories of Data Subjects

A. The subject matter and duration of the processing of Personal Data:	The subject matter and duration are set out in the Agreement
B. The nature and purpose of the processing of Personal Data:	That which is necessary to perform Services pursuant to the terms and conditions of the Agreement, as further specified in any attachments, exhibits, and any schedules thereto, and as further instructed by Controller in its use of the Services.
C. The types of Personal Data to be Processed:	Names; user profiles; contact information; unique ID (employee or student number); geo-location data; device identifiers; monitoring information, including a user's interaction with the Services; geolocation data.
D. The categories of Data Subjects to whom the Personal Data relates:	Authenticated users (employees, consumers, students).

Exhibit 2
Student Personal Data Processing Addendum

This Student Personal Data Addendum ("SDPA") by and between Scenario Learning, LLC d/b/a Vector Solutions ("Service Provider") and Client (each a "Party" and collectively the "Parties") is effectively incorporated into the Vector Solutions Education Software as a Service Agreement entered into between Service Provider and Client ("Agreement") and supplements the Data Processing Addendum ("DPA") attached thereto. This SDPA is effective as of the date of the Agreement. In the event of a conflict between any provisions of, or attachments to, the Agreement and the provisions of this SDPA, the provisions of this SDPA shall govern and control.

1. Definitions

For purposes of this SDPA,

1.1 "**Student Personal Data**" means: (1) Personal Information, as defined in the DPA, about a student attending or seeking to enroll in a school or university; (2) personally identifiable information of a student or child as defined in applicable federal or state law, such as the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g (34 C.F.R. Part 99), and the Children's Online Privacy Protection Act, 15 U.S.C. 6501-6502 (16 C.F.R. Part 312); and (3) student information as defined in state education laws that may apply, such as N.Y. Educ. Law §§ 2-c & 2-d, and any implementing regulations.

1.2 "**Teacher or Principal Data**" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals and not subject to release under a Data Protection Law.

1.3 Student Personal Data and Teacher or Principal Data are collectively referred to as "**Protected Student Data**."

All other defined terms used herein shall carry meanings set forth in the Agreement and its attachments.

2. Representations

2.1 Service Provider does not require access to or use of Protected Student Data in order to perform the Services being provided in the Agreement. As such, Client shall not upload Protected Student Data to Service Provider's platform as such data will not be encrypted at rest. To the extent that Client uploads any such Protected Student Data to the platform, such processing will be subject to the DPA.

2.2 To the extent Service Provider collects or processes Protected Student Data and qualifies as a third-party vendor or contractor under a Data Protection Law that governs Protected Student Data, Service Provider is performing an institutional service or function for which Client would otherwise use its employees, under the direct control of Client, with respect to the collection, use and maintenance of Protected Student Data.

2.3 Client is responsible for compliance with its obligations as a data controller of Protected Student Data, and in particular for justification of any transmission of Protected Student Data to Service Provider, and for obtaining any required consents and/or providing notices under applicable Data Protection Laws.

2.4 Consistent with the DPA, Service Provider, its employees, agents, and contractors, shall use Protected Student Data transmitted to it, or authorized by Client for collection by Service Provider, only for purposes set forth in the Agreement and as otherwise permitted by law, pursuant to Service Provider's capacity as a Processor acting at the direction of, and on behalf of, Client to aid in the fulfillment of Client's legitimate educational interests.

2.5 Service Provider shall treat Protected Student Data as confidential and shall inform all its employees, agents, contractors and/or subprocessors engaged in Processing Protected Student Data of the confidential nature of such data consistent with the confidentiality provisions set forth in the Agreement and DPA. Client agrees that Service Provider may engage the contractors and/or subprocessors : Amazon Web Services and Microsoft Azure.

2.6 Service Provider may transfer Protected Student Data to its employees, agents, contractors and/or subprocessors, but only to the extent necessary to carry out the Agreement. Service Provider shall not transfer Protected Student Data to any other third party.

2.7 Service Provider shall not sell (for monetary consideration), rent, or use Protected Student Data for purposes beyond that which is necessary to achieve the necessary business purposes set forth in the Agreement and DPA.

2.8 Service Provider maintains a written information security policy that complies with applicable industry standards related to the Processing of Protected Student Data.

2.9 Service Provider has provided Client with an online privacy notice at www.vectorsolutions.com/privacy-policy/ that Client can use to update its own privacy notice for purposes of disclosing the Protected Student Data collected and processed by Service Provider under this Agreement.

3. Parents' Bill of Rights for Data Privacy and Security

Service Provider acknowledges that, where it receives Protected Student Data through its relationship with the Client pursuant to this Agreement, the following applies:

3.1 A student's personally identifiable information cannot be sold or released for any commercial purposes;

3.2 Parents have the right to inspect and review the complete contents of their child's education record;

3.3 State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;

3.4 A complete list of all student data elements collected by the Client is available for public review at the Client's website or by writing to privacy@vectorsolutions.com; and

3.5 Parents have the right to have complaints about possible breaches of student data addressed. Parents should be directed to Client and Client will address such complaints. Further, inquiries, may be directed to privacy@vectorsolutions.com.

4. Supplemental Information

4.1 The exclusive purpose for which the Protected Student Data may be used is to provide Client with access to the Service(s) specified in the Agreement. Children may access and use our SafeSchools Alert Service and SafeSchools Mobile App to track, manage and resolve incidents in our web-based system. The Service and the App do not require or encourage children to provide personal information. Any information provided by the child is used to manage, track, and resolve reported incidents for the purpose of keeping children safe.

4.2 To the extent Service Provider engages any third-party contractors and/or subprocessors to perform one or more of its obligations under the Agreement and shares Protected Student Data with

such third-party contractors and/or subprocessors, Service Provider will be responsible for each such subprocessor's and/or third-party contractor's performance with respect to its data protection and security obligations.

4.3 The Initial Term is indicated in Schedule A to the Agreement. Upon expiration of the term of the Agreement (including any Renewal Terms) and upon the Client's written request, Service Provider shall destroy all copies of the Protected Student Data unless such retention is either expressly authorized for a prescribed period by the Agreement or other written agreement between the Parties, or expressly requested by Client for purposes of facilitating the transfer of Protected Student Data to Client or expressly required by law.

4.4 Consistent with the DPA, Service Provider shall assist Client in providing parents, eligible students, teachers, or principals with access to, and the ability to correct, inaccurate Student Personal Data within Service Provider's platform or control (if any). All such requests shall be directed to Client without undue delay.

4.5 Protected Student Data that Service Provider receives, if any, will be stored on systems maintained by Service Provider, or by a subcontractor and/or third party contractor under its control and supervision, in a reasonably secure data center facility located within the United States.

4.6 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Service Provider shall implement reasonable and appropriate administrative, technical and physical safeguards designed to align with the NIST Cybersecurity Framework and protect the Protected Student Data against unauthorized or unlawful Processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, destruction, or damage, including deployment of encryption technology where commercially feasible.

Vector Solutions

By: Justin Moore

Name: Justin Moore

Title: K12 Sales Director

Date: 6/22/21

Client

By: RJ DeLisle

Name: RJ DeLisle

Title: Data Privacy Officer

Date: 1-31-2023