DATA PRIVACY AGREEMENT

Medina Center School District

And

Vista Higher Learning, Inc.

This Data Privacy Agreement ("DPA") is by and between the Medina Central School District ("EA"), an Educational Agency, and Vista Higher Learning, Inc. ("Contractor"), collectively, the "Parties."

RECITALS

WHEREAS, the Contractor has agreed to provide the EA with certain services ("Services") pursuant to a contract dated 10/15/2020 and expires on 10/31/2026 ("Service Agreement"); and

WHEREAS, in order to provide the Services, the Contractor may receive from the EA and the EA may provide the Contractor student data, teacher and/or principal data (collectively, "Protected Data"), protected by several New York and federal laws and regulations, among them, the Federal Educational and Privacy rights Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); Education Law § 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the laws referred to above.

NOW THEREFORE, the Parties agree as follows:

ARTICLE I: DEFINITIONS

As used in this agreement, the following terms shall have the following meanings:

1. **Authorized Users:** Contractor's employees and non-employee recipients.
2. **Breach:** The unauthorized acquisition, access, use, or disclosure of Protected Data by or to a person not authorized to acquire, access, use, or receive it.

3. **Commercial or Marketing Purpose:** The sale of student data, teacher or principal data, or its use or disclosure, whether directly or indirectly, to derive a profit, for advertising purposes or to develop, improve or market products or services to students.
4. **Contract, agreement or written agreement**: A binding agreement between an EA and a third-party, which shall include but not be limited to an agreement created in electronic form and signed with an electronic or digital signature or a click wrap agreement that is used with software licenses, downloaded and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.
5. **Disclose**: To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
6. **Education Record:** An education record as defined in FERPA and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
7. **Educational Agency**: A school district, board of cooperative educational services, school, charter school or the New York State Education Department.
8. **Eligible Student:** A student eighteen years or older.
9. **Encrypt or Encryption**: Methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process or key that might enable decryption has not been breached, as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304.
10. **Non-Employee Recipients:** Contractor's nonemployee agents, consultants and/or subcontractors engaged in the provision of Services pursuant to the Service Agreement.
11. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
12. **Parent:** A parent, legal guardian or person in parental relation to the student.
13. **Release:** Shall have the same meaning as Disclose.
14. **Student:** Any person attending or seeking to enroll in an educational agency.
15. **Student Data:** Personally identifiable information, as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, regarding students from the student records of an educational agency. For the avoidance of doubt, Student Data does not include information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Service Provider's services.

16. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
17. **Teacher or Principal Data**: Personally identifiable information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law § 2012(c).

ARTICLE II: DATA PROTECTION

1. **Purpose.** Contractor is permitted to have access to Protected Data solely and exclusively for the purpose set forth in the Service Agreement as outlined in Exhibit B, bill of rights for data privacy and security, supplemental information for contracts that utilize protected data. Contractor agrees to hold the Protected Data in strict confidence, and not to disclose it for the benefit of another or for any use or purpose other than for providing the Services. The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this Agreement.
2. **Ownership of Protected Data**. Contractor has no property or licensing rights or claims of ownership to any Protected Data.
3. **Right to Review.** The EA has the right to review Contractor's procedures, practices and controls related to the protection of Protected Data as provided in the Contractor's Data Security and Privacy Plan. To that end, upon request, Contractor will make available for review policies, procedures, practices and documentation related to the protection of Protected Data. In addition, in the event of reports of breaches of unauthorized releases of student data or teacher or principal data by the Contractor, the Contractor will cooperate with the EA and the state Chief Privacy Officer who is authorized, based upon such reports, to conduct an investigation including requiring the Contractor to submit documentation, provide testimony, and/or allow for the inspection of the Contractor's facilities and records, in connection with the Protected Data.
4. **Parent and Eligible Student Access.** Education Law §2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within twenty-five (25) calendar days to the EA's requests for the Contractor to facilitate such review by a Parent or Eligible Student, and as applicable, facilitate corrections as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall immediately notify the EA and refer the Parent or Eligible Student to the EA.

5. **Compliance with Law**. Contractor agrees to maintain the confidentiality of Protected Data in accordance with applicable New York and federal laws, rules, and regulations including, but not limited to, FERPA; COPPA; PPRA; IDEA; Education Law § 2-d; 8 NYCRR Part 121; and EA policies relating to data privacy and security as amended, including, without limitation, those data privacy and security policies that are implemented subsequent to the execution of this DPA and which are provided to Contractor.
6. **Bill of Rights for Data Privacy and Security**. As required by §2-d of the Education Law, the parents' bill of rights for data privacy and security and bill of rights with supplemental information for contracts that utilize personally identifiable information are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Pursuant to Education Law §2-d, the EA is required to post the completed Exhibit B on its website.
7. **Contractor's Authorized Users**. Contractor shall only disclose Protected Data to Authorized Users who need to know the Protected Data in order to carry out the Services, provided that such disclosure shall be made only to the extent justifiable by such need, and shall adopt and maintain administrative, physical and technical security and privacy controls and protocols that ensure access only to Authorized Users. Contractor shall ensure that all such Authorized Users comply with the terms of this DPA. Contractor shall ensure that each Non-Employee Recipient is contractually bound by an agreement that includes confidentiality and data security obligations equivalent to, and no less protective than, those found in this DPA.
8. **Subcontractor.** Where use of a subcontractor is authorized, Contractor shall, by written agreement, ensure that all requirements set forth herein apply to all subcontractors performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to Protected Data. Contractor shall take full responsibility for the acts and omissions of its subcontractors in relation to its provisions of the services to the EA under the Service Agreement. Contractor shall ensure that all its subcontractors, similar to its employees and assignees, who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.
9. **Destruction of Data**. Nothing in the Service Agreement shall authorize Contractor to maintain Protected Data after termination of the Service Agreement. Contractor shall provide the EA a written certification of the secure deletion and/or destruction of Protected Data held by the Contractor and its Non-Employee Recipients no later than thirty (30) business days after the Service Agreement terminates. If applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer, in a format agreed to by the parties, Protected Data to the EA, at the EA's option and written direction provided to the Contractor prior to or immediately upon the expiration or termination of the Service Agreement. Contractor shall thereafter, with regard to all Protected Data (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all

Protected Data maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Non-Employee Recipients , securely delete and/or destroy such Protected Data in a manner that does not allow it to be retrieved or retrievable, read or reconstructed, and direct its Non-Employee Recipients to do the same. Contractor shall ensure that no copy, summary or extract of the Protected Data is retained on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever by Contractor or its Non-Employee Recipients. Hard copy media must be shredded or destroyed such that Protected Data cannot be read or otherwise cannot be reconstructed, and electronic media must be cleared, purged, or destroyed such that the Protected Data cannot be retrieved. Redaction is specifically excluded as a means of data destruction.

10. **No Sale or Commercial Use**. Contractor agrees that it will not sell or use PII for a Commercial or Marketing Purpose except as authorized in the Service Agreement.
11. **Disclosure Limitations.** Unless as permitted by this DPA, Contractor shall not disclose any Protected Data to any party who is not an Authorized User. Notwithstanding the foregoing, Contractor may disclose Protected Data if such disclosure is required by statute or court order and the Contractor makes a reasonable effort to notify the EA of the order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the Protected Data is disclosed, unless such disclosure to the EA is expressly prohibited by statute or court order.
12. **Encryption.** Contractor shall use industry standard practices to preserve and protect Protected Data from unauthorized disclosure. Contractor shall use Encryption technologies to protect Protected Data at rest and in transit/motion.
13. **Data Security and Privacy Plan**. Contractor shall maintain reasonable administrative, technical and physical safeguards that conform to federal, State and EA mandates, the NIST Cybersecurity Framework or an equivalent standard that meets and or exceeds its requirements, and generally recognized industry standards and practices to protect the security, confidentiality and integrity of Protected Data in its custody. Contractor is required to have a Data Privacy and Security Plan that, at a minimum, complies with 8 NYCRR Part 121. Contractor's data privacy and security safeguards are described in Exhibit C, Contractor's Data Privacy and Security Plan.
14. **Training**. Contactor shall ensure that all Authorized Users who have access to Protected Data have received or will receive training on the federal and state laws governing confidentiality of such data and understand the privacy and data security obligations of this DPA prior to receiving access.
15. **Data Breach Reporting**. Contractor shall without unreasonable delay notify the EA of any breach of security resulting in an unauthorized release or disclosure of Protected Data by

Contractor or its Authorized Users in violation of applicable state or federal law and/or this DPA in the most expedient way possible, but no later than three (3) business days after discovery of the breach or unauthorized release. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, at the address set forth on Exhibit B. Such notification shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include a brief description of the breach or unauthorized release; the dates of the incident and the date of discovery, if known; a description of the types of Personally Identifiable Information affected, an estimate of the number of records affected, a brief description of the Contractor's investigation or plan to investigate, and contact information for representatives who can assist the EA. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The breach and unauthorized release of certain Personally Identifiable Information protected by Education Law Section 2-d may subject the Contractor to additional penalties.

16. **Cooperation with Investigations.** Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, to protect the integrity of any investigations into a breach or unauthorized release of Protected Data. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor.
17. **Notification Costs.** Where a breach or unauthorized release of Protected Data occurs that is attributable to Contractor or any of its Authorized Users, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to parents, students, teachers, and/or principals, in accordance Education Law § 2-d and 8 NYCRR Part 121.

ARTICLE III: MISCELLANEOUS

1. **Priority of Agreements and Precedence.** In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein, the Service Agreement, and any of Contractor's terms of service or privacy notices that apply to the Services, the terms and conditions of this DPA shall prevail. In addition, this DPA and all its Exhibits shall be deemed a part of and incorporated into the Service Agreement but shall survive the termination of the Service Agreement in the manner set forth herein.
2. **Entire Agreement**. This DPA constitutes 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.
3. **Governing Law; Venue and Jurisdiction.** This DPA will be governed by and construed in accordance with the laws of the state of New York, without regard to conflicts of law principles.

The state and federal courts located in New York will have exclusive jurisdiction to adjudicate any dispute arising out of or relating to this DPA, the Service Agreement referenced in this DPA, or the transactions contemplated hereby.

4. **Execution.** This DPA as well as attached Exhibits A, B and C may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document. This DPA as well as the attached exhibits A, B and C may be executed by signatures to facsimile copy or electronic transmittal documents in lieu of an original or machine generated or copied document, and each signature thereto shall be and constitute an original signature, as if all Parties had executed a single original document.

VISTA HIGHER LEARNING, INC.

Signature: Jon Aram Digitally signed by Jon Aram Date: 2020.12.11 13:56:40 -05'00'

Printed Name: Jon Aram

Title/Position: CEO

Date: 12/11/2020

MEDINA CENTRAL SCHOOL DISTRICT

Signature:

Printed Name: Anthony Moreno

Title/Position: Data Protection Officer

Date: 12/7/2020

Education Law §2-d Bill of Rights for Data Privacy and Security Education Law §2-d Bill of Rights for Data Privacy and Security

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Medina Central School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

2) Parents have the right to inspect and review the complete contents of their child's education record.

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.

4) A complete list of all student data elements collected by New York State is available for public review at the following website http://www.nysed.gov/data-privacy-security/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.

5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website http://www.nysed.gov/data-privacy-security/report-improper-disclosure

APPENDIX

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Medina Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

1) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract; Page 2 of 2

2) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including

but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);

3) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);

4) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

5) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and

6) Address how the data will be protected using encryption while in motion and at rest.

VISTA HIGHER LEARNING, INC.
Signature: Jon Aram Digitally signed by Jon Aram Date: 2020.12.11 13:57:09 -05'00'
Printed Name: Jonathan Aram
Title: CEO
Date: 12/11/2020

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Vista Higher Learning, Inc.
Description of the purpose(s) for which Contractor will receive/access PII	The provision of educational content, access to Service Provider's digital platform, courseware, customizing learning, and related digital educational services.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date: October 15, 2020 Contract End Date: October 31, 2026
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely delete and destroy data.

Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, Contractor will work with the EA to facilitate such corrections, as applicable.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Sensitive data is encrypted at rest.
Encryption	Data will be encrypted while in motion and at rest.

VISTA HIGHER LEARNING, INC.	
Signature:	Jon Aram Digitally signed by Jon Aram Date: 2020.12.11 13:58:01 -05'00'
Printed Name:	Jon Aram
Title:	CEO
Date:	12/11/2020

EXHIBIT C

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York State. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Provided for in Section 4 of the VHL Data Security and Privacy Plan.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Provided for in Section 6 of the VHL Data Security and Privacy Plan.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Provided for in Section 6(d) of the VHL Data Security and Privacy Plan.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Provided for in Section 6(d) of the VHL Data Security and Privacy Plan.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Provided for in Section 6(e) of the VHL Data Security and Privacy Plan.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	See Article II, paragraph 9 of the DPA.
7	Describe your secure destruction practices and how certification will be provided to the EA.	See Article II, paragraph 9 of the DPA.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Provided for in the VHL Data Security and Privacy Plan.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 https://www.nist.gov/cyberframework/new-framework	Provided for in the VHL Data Security and Privacy Plan.
