DATA PRIVACY AGREEMENT

MEDINA CENTRAL SCHOOL DISTRICT

and

CORAdvantage

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

ARTICLE I: DEFINITIONS

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

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.

2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.

3. **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.

4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

5. **Educational Agency**: As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.

6. **Eligible Student:** A student who is eighteen years of age or older.

7. **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

9. **Parent:** A parent, legal guardian or person in parental relation to the Student.

10. **Personally Identifiable Information (PII):** Means 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 , and Teacher or Principal APPR Data, as defined below.

11. **Release:** Shall have the same meaning as Disclose.

12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.

13. **Student:** Any person attending or seeking to enroll in an Educational Agency.

14. **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.

15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.

16. **Teacher or Principal APPR 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 §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated 7/1/2023 to until this agreement expires ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy 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); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. **Authorized Use.**

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. **Data Security and Privacy Plan**.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. **EA's Data Security and Privacy Policy**

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

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).

CORAdvantage	
Description of the purpose(s) for which Contractor will receive/access PII	COR Advantage uses PII data to provide analysis of student assessment data.
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR Data
Contract Term	Contract Start Date ___7/1/2023 _____ Contract End Date The parties reserve the right to renew the contract
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 transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • 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, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.

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: All production servers are maintained with the latest virus protection and malware updates. All production servers are connected through a monitored firewall device. IP addresses of production servers are not visible via the internet. The entire network is automatically monitored 24 hours per day, 7 days per week, 365 days per year.
Encryption	Data will be encrypted while in motion and at rest.

CORAdvantage
Signature: KSC
Print Name: Katie Schmieg
Title: VP of Operations
Date: 4/3/2023

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 or provide a plan 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.	We're committed to helping customers and users understand, and where applicable, comply with the General Data Protection Regulation (GDPR). The GDPR is the most comprehensive EU data privacy law in decades, and went into effect on May 25, 2018. (COR Advantage GDPR Commitment)
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	We have put in place appropriate security measures to prevent your Personal Data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. We limit access to your Personal Data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your Personal Data on our instructions and they are subject to a duty of confidentiality (COR Advantage Privacy Policy)
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.	Employees will be familiar the rules and rights listed around both the End User License Agreement as well as Terms & Policies.
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.	Each Party represents and warrants to the other Party that it will: (a) comply with all laws, regulations and governmental orders applicable to its organization in the performance of this EULA, and in the use of the Services and Platform; (b) it has the full power and authority to enter into and fully perform its obligations under this EULA; and (c) it is duly organized under and existing under the laws of its territory of organization. (COR Advantage Terms of Service)
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.	We have put in place procedures to deal with any suspected Personal Data breach and will notify you and any applicable regulator of a breach where we are legally required to do so. (CORAdvantage Privacy Policy)
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	The customer is the sole and exclusive owner of data created by its use, and its Authorized Users' use, of the Platform and Services. We will only retain your Personal Data for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Request erasure of your Personal Data. This enables you to ask us to delete or remove Personal Data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your Personal Data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your Personal Data to comply with local law.
8	Outline how your data security and privacy program/ practices align with the EA's applicable policies.	All production servers are maintained with the latest virus protection and malware updates. All production servers are connected through a monitored firewall device. IP addresses of production servers are not visible via the internet. The entire network is automatically monitored 24 hours per day, 7 days per week, 365 days per year.

9	Outline how your data security and privacy program/ practices materially align with the NIST Cybersecurity Framework Version 1.1.	N/A