CONFIDENTIALITY AND DATA SECURITY AND PRIVACY STANDARDS ADDENDUM

This Addendum made this _____ day of _____, 2024 to the Agreement by and between [TYPE OUT VENDOR NAME]_____ ("VENDOR") having its principal place of business at _____, and RYE CITY SCHOOL DISTRICT (the "SCHOOL DISTRICT"), having its principal place of business at 555 Theodore Fremd Avenue, Suite B-101, Rye, New York 10580.

WHEREAS, VENDOR will receive "student data" as that term is defined in New York Education Law § 2-d and the regulations promulgated thereunder (hereinafter referred to as "Educ. Law § 2-d"); and

WHEREAS, both SCHOOL DISTRICT and VENDOR are desirous of fulfilling their respective obligations under Educ. Law § 2-d and the regulations promulgated thereunder.

NOW, THEREFORE, in consideration of the mutual promises and covenants contained in the Agreement, the parties hereto mutually agree as follows:

1. VENDOR, its employees, and/or agents agree that all information obtained in connection with the services provided for in this Agreement is deemed confidential information. VENDOR, its employees, and/or agents shall not use, publish, discuss, disclose or communicate the contents of such information, directly or indirectly with third parties, except as provided for in this Agreement. VENDOR further agrees that any information received by VENDOR, its employees, and/or agents during the course of the services provided pursuant to this Agreement which concerns the personal, financial, or other affairs of SCHOOL DISTRICT, its employees, agents, clients, and/or students will be treated by VENDOR, its employees, and/or agents in full confidence and will not be revealed to any other persons, firms, or organizations.

2. VENDOR acknowledges that it may receive and/or come into contact with personally identifiable information, as defined by Educ. Law § 2-d, from records maintained by SCHOOL DISTRICT that directly relate to a student(s) (hereinafter referred to as "education record"). VENDOR understands and acknowledges that it shall have in place sufficient protections and internal controls to ensure that information is safeguarded in accordance with applicable laws and regulations, and understands and agrees that it is responsible for complying with state data security and privacy standards for all personally identifiable information (hereinafter referred to as "PII") from education records, and it shall:

   a. limit internal access to education records to those individuals that are determined to have legitimate educational interests;

   b. not use the education records for any purposes other than those explicitly authorized in this Agreement;

   c. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of education records in its custody; and

d. use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5 and the National Institute of Standards and Technology Cyber Security Framework Version 1.1.

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

4. VENDOR further understands and agrees that it is responsible for submitting a data security and privacy plan to SCHOOL DISTRICT prior to the start of the term of this Agreement. Such plan shall outline how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract consistent with SCHOOL DISTRICT's policy on data security and privacy, as adopted. Further, such plan shall include a signed copy of SCHOOL DISTRICT's Parents' Bill of Rights and the training requirement established by VENDOR for all employees who will receive PII from student records (hereinafter referred to as "student data").

5. VENDOR understands that as part of SCHOOL DISTRICT's obligations under Educ. Law § 2-d, VENDOR is responsible for providing SCHOOL DISTRICT with supplemental information to be included in SCHOOL DISTRICT's Parents' Bill of Rights. Such supplemental information shall be provided to SCHOOL DISTRICT within ten (10) days of execution of this Agreement and shall include:

a. the exclusive purposes for which the student data will be used;

b. how VENDOR will ensure that subcontractors, persons or entities that VENDOR will share the student data with, if any, will abide by data protection and security requirements;

c. that student data will be returned or destroyed upon expiration of the Agreement;

d. if and how a parent, student, or eligible student may challenge the accuracy of the student data that is collected; and

e. where the student data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

6. Upon request by SCHOOL DISTRICT, VENDOR shall provide SCHOOL DISTRICT with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate VENDOR's own information security policies, confidentiality obligations, and applicable laws. In addition, VENDOR may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, SCHOOL DISTRICT's

policies applicable to VENDOR, and alignment with the NIST Cybersecurity Framework performed by an independent third party at VENDOR's expense, and provide the audit report to SCHOOL DISTRICT. VENDOR may provide SCHOOL DISTRICT with a recent industry standard independent audit report on VENDOR's privacy and security practices as an alternative to undergoing an audit.

7. The following requirements apply if VENDOR will use subcontractors that have access to PII in the course of providing the services:

a. VENDOR shall only disclose PII to VENDOR's employees and subcontractors who need to know the PII in order to provide the services and the disclosure of PII shall be limited to the extent necessary to provide such services. VENDOR shall ensure that all such employees and subcontractors comply with the terms of this addendum.

b. VENDOR must ensure that each subcontractor performing functions pursuant to the Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this addendum.

c. VENDOR shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this addendum, VENDOR shall: notify SCHOOL DISTRICT and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this addendum. In the event there is an incident in which the subcontractor compromises PII, VENDOR shall follow the data breach reporting requirements set forth herein.

d. VENDOR shall take full responsibility for the acts and omissions of its employees and subcontractors.

e. VENDOR must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and VENDOR makes a reasonable effort to notify SCHOOL DISTRICT of the court order or subpoena in advance of compliance but in any case, provides notice to SCHOOL DISTRICT no later than the time the PII is disclosed, unless such disclosure to SCHOOL DISTRICT is expressly prohibited by the statute, court order or subpoena.

8. VENDOR shall ensure that all its employees and subcontractors 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. In the event of a breach of the within confidentiality and data security and privacy standards provision and unauthorized release of student data, VENDOR shall immediately notify SCHOOL DISTRICT and advise it as to the nature of the breach and steps VENDOR has taken to minimize said breach. Said notification must be made within seven (7) days of the breach.

Notifications required pursuant to this section must be in writing, given by personal delivery, or by registered or certified, and must to the extent available, and shall include a description of the breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of VENDOR's investigation; and the contact information for representatives who can assist SCHOOL DISTRICT. In the case of required notification to a parent or eligible student, VENDOR shall promptly reimburse SCHOOL DISTRICT for the full cost of such notification.

10. VENDOR agrees that it will cooperate with SCHOOL DISTRICT and law enforcement, where necessary, in any investigations into a breach. Any costs incidental to the required cooperation or participation of VENDOR or its' Authorized Users, as related to such investigations, will be the sole responsibility of VENDOR if such breach is attributable to VENDOR or its subcontractors.

11. In the event that VENDOR fails to notify SCHOOL DISTRICT of a breach, said failure shall be punishable by a civil penalty of the greater of $5,000 or up to $20 per student, teacher and principal whose data was released, provided that the maximum penalty imposed shall not exceed the maximum penalty imposed under General Business Law, section 899-aa(6)(a).

12. Except as set forth in paragraph 11, above, in the event VENDOR violates Education Law 2-d, said violation shall be punishable by a civil penalty of up to $1,000. A second violation involving the same data shall be punishable by a civil penalty of up to $5,000. Any subsequent violation involving the same data shall be punishable by a civil penalty of up to $10,000. Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

13. VENDOR shall indemnify and hold SCHOOL DISTRICT harmless from any claims arising from its breach of the within confidentiality and data security and privacy standards provision.

14. The following procedure shall take place upon the termination of the Agreement:

a. VENDOR agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing services to SCHOOL DISTRICT, 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 SCHOOL DISTRICT for purposes of facilitating the transfer of PII to SCHOOL DISTRICT or expressly required by law. As applicable, upon expiration or termination of the Agreement, VENDOR shall transfer PII, in a format agreed to by the parties to SCHOOL DISTRICT.

b. If applicable, once the transfer of PII has been accomplished in accordance with SCHOOL DISTRICT's written election to do so, VENDOR agrees to return or destroy all PII when the purpose that necessitated its receipt by VENDOR has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies,

archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of VENDOR in a secure data center and/or cloud-based facilities that remain in the possession of VENDOR or its subcontractors, VENDOR shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

c. VENDOR shall provide SCHOOL DISTRICT with a written certification of the secure deletion and/or destruction of PII held by VENDOR or its subcontractors.

d. To the extent that VENDOR and/or its subcontractors continue to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

15. The parties further agree that the terms and conditions set forth herein shall survive the expiration and/or termination of this Agreement.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement the day and year first above written.

RYE CITY SCHOOL DISTRICT
BOARD OF EDUCATION

Date:_____ By: _____

[TYPE OUT VENDOR NAME]

Date:_____ By: _____