Appendix 1

Data Protection Addendum

This Data Protection Addendum ("**Addendum**") is incorporated into and made a part of the Master Agreement between Mindex ("**Mindex**" or "**Vendor**") and Customer (the "**Agreement**") to to provide for compliance with the requirements of New York Education Law 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "**Section 2-d**"). Any capitalized terms not defined herein will have the meaning given to them in the Agreement.

1. **Definitions.**
    a. Personally Identifiable Information: For purposes of this Addendum, Personally Identifiable Information has the meaning ascribed to it in Section 2-d.
2. **Vendor Obligations**. In addition to Vendor's' obligations under the Agreement, Vendor will:
    a. Comply with Customer's data security and privacy policy as provided to Vendor and comply with Section 2-d;
    b. Limit internal access to Personally Identifiable Information to only those employees or sub-contractors that need access to provide the services under the Agreement;
    c. Not use the Personally Identifiable Information for any purpose not explicitly authorized in the Agreement and this Addendum thereto;
    d. Except as permitted by applicable law, including Section 2-d, not disclose any Personally Identifiable Information to any other party without the prior written consent of the parent or eligible student;
    e. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality, and integrity of Personally Identifiable Information in Vendor's custody;
    f. Promptly notify Customer of any breach or unauthorized release of Personally Identifiable Information without unreasonable delay, but no more than seven (7) days after Vendor has confirmed or been informed of the breach or unauthorized release. Vendor will not be liable for any damages or costs incurred by the Customer in responding to a security breach or any loss or theft of Personally Identifiable Information unless, and only to the extent, such breach is attributable to Vendor's (or Vendor's personnel's) failure to comply with the Agreement and this Addendum thereto or otherwise due to Vendor's acts or omissions;
    g. Use commercially reasonable encryption to protect Personally Identifiable Information in Vendor's custody while in motion or at rest;
    h. Not sell Personally Identifiable Information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;
3. **Data Security and Privacy Plan**

a. **Compliance.** In order to implement all relevant state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with Customer's data security and privacy policy, Vendor will:

   i. Follow policies and procedures compliant with (i) relevant state, federal, and local data security and privacy requirements, including Section 2-d, (ii) this Addendum, and (iii) Customer's data security and privacy policy;

   ii. Implement commercially reasonable administrative, technical, operational, and physical safeguards and practices to protect the security of Personally Identifiable Information in accordance with relevant law;

   iii. Follow policies compliant with Customer's Parents' Bill of Rights and Parents' Bill of Rights Supplemental Information, attached as Attachment 1 and 2 to this Addendum and incorporated by reference herein;

   iv. Annually train its officers and employees who have access to Personally Identifiable Information on relevant federal and state laws governing confidentiality of Personally Identifiable Information; and

   v. In the event any subcontractors are engaged in relation to this Agreement, manage relationships with sub-contractors to contract with sub-contractors to protect the security of Personally Identifiable Information in accordance with relevant law.

b. **Safeguards.** To protect Personally Identifiable Information that Vendor receives under the Agreement, Vendor will follow policies that include the following administrative, operational, and technical safeguards:

   i. Vendor will identify reasonably foreseeable internal and external risks relevant to its administrative, technical, operational, and physical safeguards;

   ii. Vendor will assess the sufficiency of safeguards in place to address the identified risks;

   iii. Vendor will adjust its security program in light of business changes or new circumstances;

   iv. Vendor will regularly test and monitor the effectiveness of key controls, systems, and procedures; and

   v. Vendor will protect against the unauthorized access to or use of personally identifiable information.

c. **Training.** Officers or employees of Vendor who have access to Personally Identifiable Information will receive training annually on the federal and state laws governing confidentiality of such data prior to receiving access.

d. **Subcontractors.** Vendor will utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the Agreement. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the Agreement, it will implement policies to manage those relationships in accordance with applicable laws and will obligate its subcontractors to protect Personally Identifiable Information in all contracts with

such subcontractors, including by obligating the subcontractor to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations and the Agreement.

e. **Data Security and Privacy Incidents.** Vendor will manage data security and privacy incidents that implicate Personally Identifiable Information, including identifying breaches and unauthorized disclosures, by following an incident response policy for identifying and responding to incidents, breaches, and unauthorized disclosures. Vendor will notify Customer of any breaches or unauthorized disclosures of Personally Identifiable Information promptly but in no event more than seven (7) days after Vendor has discovered or been informed of the breach or unauthorized release.

f. **Effect of Termination or Expiration**. Vendor will implement procedures for the return, transition, deletion and/or destruction of Personally Identifiable Information at such time that the Agreement is terminated or expires.

4. **Conflict.** All terms of the Agreement remain in full force and effect. Notwithstanding the foregoing, to the extent that any terms contained within the Agreement, or any terms contained within any schedules attached to and made a part of the Agreement, conflict with the terms of this Addendum, the terms of this Addendum will apply and be given effect.

ATTACHMENT A
Parent's Bill of Rights for Data Security and Privacy

Albany-Schoharie-Schenectady-Saratoga BOCES (BOCES) is committed to protecting the privacy and security of personally identifiable information about students who attend BOCES instructional programs in accordance with applicable law, including New York State Education Law Section 2-d.

To further these goals, BOCES wishes to inform parents 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 the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863
EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints may be directed to the NYS Chief Privacy Officer by writing to the New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be directed to the Chief Privacy Officer via email at: CPO@mail.nysed.gov.

BY THE VENDOR:

Marc Fiore
Signature

President
Title

10/21/2024
Date

ATTACHMENT B

Supplemental Information About the Agreement Between Customer and Mindex Technologies, Inc.

1. **Exclusive Purpose**. Vendor will use the Personally Identifiable Information to which it is provided access for the exclusive purpose of providing Vendor's services as more fully described in the Agreement. Vendor agrees that it will not use the Personally Identifiable Information for any other purposes not explicitly authorized in the Agreement.
2. **Subcontractors**. In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the Agreement, Vendor will obligate its subcontractors, assignees, or other authorized persons or entities to whom it discloses Personally Identifiable Information, to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations, by requiring its subcontractors to agree in their contracts with Vendor to such data protection obligations imposed on Vendor by state and federal laws and regulations (e.g., FERPA; Education Law §2-d) and this Agreement.
3. **Agreement Term & Termination**.
    a. The Agreement commences on the Effective Date of the Agreement and expires on the earlier of (i) Vendor no longer providing services to Customer and (ii) termination of the Agreement in accordance with its terms.
    b. Vendor will implement procedures for the return, deletion, and/or destruction of Personally Identifiable Information at such time that the Agreement is terminated or expires.
4. **Challenging Accuracy of Personally Identifiable Information**. Parents or eligible students can challenge the accuracy of any Personally Identifiable Information provided by a Customer to Vendor by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to MINDEX by following the appeal process in their employing school district's applicable APPR Plan.
5. **Data Storage and Security Protections**.
    a. **General**. Any Personally Identifiable Information Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility. Vendor will maintain reasonable administrative, technical and physical safeguards in accordance with 2-d to protect the security, confidentiality, and integrity of Personally Identifiable Information in Vendor's custody.
    b. **Encryption**. Vendor will encrypt data in motion and at rest using methodology in accordance with 2-d.