Exhibit B

Data Protection Addendum

This Data Protection Addendum ("Addendum") is incorporated into and made a part of the Master Agreement between Mindex ("Contractor") and OCM BOCES ("Agreement") to to provide for compliance with the requirements of New York Education Law Section 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. For the avoidance of doubt, the parties acknowledge and agree that Vendor does not have access to teacher or principal data as those terms are defined in Section 2-d.

2. **Vendor Obligations**. In addition to Vendor's' obligations under the Agreement and this Addendum, Vendor will:
    a. Comply with Customer's data security and privacy policy as provided to Vendor and 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; and
    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 the educational agency'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 Appendices A and B 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 student data, or teacher or principal data receive or will receive training annually on the federal and state laws governing confidentiality of such data prior to receiving access.

d. **Subcontractors.** Vendor will not 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 confidential data 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.

APPENDIX A: PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

OCM BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, OCM BOCES wishes to inform the community of the following:

1. A student's Personally Identifiable Information (PII) cannot be sold or released for any commercial or marketing purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record. This right of inspection is consistent with the requirements of the Family Educational Rights and Privacy Act (FERPA). In addition to the right of inspection of the educational record, Education Law §2-d provides a specific right for parents to inspect or receive copies of any data in the student's educational record.

3. State and federal laws protect the confidentiality of PII, 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 parents may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

5. Parents have the right to file complaints with OCM BOCES/CNYRIC about possible privacy breaches of student data by OCM BOCES/CNYRICs third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints regarding student data breaches should be directed to: OCM BOCES/CNYRIC, 6075 East Molloy Road, PO Box 4866, Syracuse, NY 13221. Phone: 315-433-8300; e-mail: pmazzaferro@cnyric.org.

6. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email: CPO@mail.nysed.gov.

APPENDIX B

Supplemental Information to Parents Bill or Rights for Data Privacy and Security:

1. The exclusive purpose for which Contractor is being provided access to Personally Identifiable Information is to provide implementation, training, maintenance and support for SchoolToolTM software. Contractor does not monitor or use Personally Identifiable Information for any reason other than as part of providing our services.

2. Student data received by Contractor, or by any assignee of Contractor, will not be sold or used for marketing purposes.

3. Contractor agrees that any of its officers or employees who have access to Personally Identifiable Information will receive training on the federal and state law governing confidentiality of such data prior to receiving access to that data which shall include but not be limited to security awareness training to all staff on topics, including Personally Identifiable Information and requirements under New York State law.

4. The agreement between Contractor and OCM BOCES for application programing interface and data exchange services expires on June 30, 2021 and shall automatically renew for one (1) year successor terms unless terminated by the Parties in accordance with the terms of the Agreement. Upon expiration or termination of the agreement, without a successor agreement in place, Contractor will assist OCM BOCES in exporting any and all student data previously received by Contractor back to OCM BOCES. Contractor will thereafter securely delete any and all student data remaining in its possession (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data), as well as any and all student data maintained on its behalf of in secure data center facilities. Contractor will ensure that no copy, summary, or extract of the student data are retained on any storage medium whatsoever by Contractor or the aforementioned secure data center facilities. Any and all measures related to the extraction, transmission, deletion, or destruction of student data will be completed within thirty (30) days of the expiration of the agreement between BOCES and Contractor. To the extent that Contractor may continue to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), they/it will not attempt to re-identify de-identified data.

5. In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by the OCM BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

6. Student data transferred to Contractor will be stored in electronic format on systems maintained by Contractor in a secure data center facility, or a data facility maintained by OCM BOCES, in the United States. In order to protect the privacy and security of student data stored in that manner, Contractor will take measures aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures may include, as required by applicable law, but are not necessarily limited to disk encryption, file encryption, firewalls, and password protection.

7. Any student data possessed by Contractor will be protected using encryption technology while in motion, in its custody and at rest.

Acknowledged and agreed to by Contractor:

Signature: Marc Fiore

Name: Marc C Fiore

Title: President

Date: 8/21/2020

OCMBOCES

Elizabeth Buselli <ebuselli@ocmboces.org>

Fwd: Introductions & Mindex MSA

Phillip Grome <pgrome@ocmboces.org>
To: Elizabeth Buselli <ebuselli@ocmboces.org>

Mon, Aug 24, 2020 at 10:30 AM

---------- Forwarded message ---------
From: **Joseph Bufano** <jbufano@ocmboces.org>
Date: Mon, Aug 24, 2020 at 8:45 AM
Subject: Fwd: Introductions & Mindex MSA
To: Phillip Grome <pgrome@ocmboces.org>, Pamela Mazzaferro <pmazzaferro@cnyric.org>, Eric Pollard <epollard@cnyric.org>

Phil,

The attached agreement is ready for execution. Can you please sign and send back a copy to Pam and I? Thank you.

Sincerely,

Joe
Joseph J. Bufano, Esq.| Director of Human Resources/School Attorney
Onondaga Cortland Madison Board of Cooperative Educational Services
Syracuse, New York | 315.433.2631| jbufano@ocmboces.org

OCMBOCES

Committed to Your Success

---------- Forwarded message ---------
From: **Allison Prout** <aprout@beckage.com>
Date: Mon, Aug 24, 2020 at 8:38 AM
Subject: RE: Introductions & Mindex MSA
To: Joseph Bufano <jbufano@ocmboces.org>
Cc: Marc Fiore <marc@mindex.com>, Dan Greene <dgreene@beckage.com>

Hi Joe,

Thank you for updating the document. I have attached a signed copy to this email and ask that you provide countersignature at your earliest convenience.