Exhibit B

Data Confidentiality and Sharing Agreement

This Data Protection Addendum ("Addendum") is incorporated into and made a part of the Master Agreement between Mindex and Customer ("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.

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, including practices that align with the NIST Cybersecurity Framework;
   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. Where a breach or unauthorized release or Personally Identifiable Information is attributed to Vendor, the Vendor shall pay for or promptly reimburse promptly reimburse Customer for the full cost of notification required under Section 2-d. Notwithstanding the foregoing, 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 using methodology specified or permitted 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 or as otherwise permitted by Section 2-d; 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 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 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**. Upon termination or expiration of the Agreement, Vendor will delete Personally Identifiable Information within its possession within thirty (30) days.

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

ULSTER COUNTY BOCES

Parents Bill of Rights - Data Privacy & Security

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

1. A student's personally identifiable information cannot be sold or released for any marketing or 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 here**, 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 should be directed in writing to:

Ulster BOCES
175 Route 32 North
New Paltz, New York 12561

or

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234

Complaints may also be directed to the
Chief Privacy Officer (CPO) via email at
CPO@mail. nysed.gov

6. The District Superintendent shall develop regulations to ensure compliance with all state and federal laws and regulations regarding the protection and security of student data and teacher or principal data.

Signature: Marc C Fi

Print Name: Marc C Fiore

Title: President

Company Name: Mindex

Date: 10/23/2020

IRAN DIVESTMENT ACT OF 2012 CERTIFICATION

As a result of the Iran Divestment Act of 2012 (Act), Chapter 1 of the 2012 Laws of New York, added new provisions to the State Finance Law (SFL), §165-a and General Municipal Law (GML) §103-g effective April 12, 2012. Under the Act, the Commissioner of the Office of General Services (OGS) will be developing a list (prohibited entities list) of "persons" who are engaged in "investment activities in Iran" (both are defined terms in the law). Pursuant to SFL § 165-a(3)(b) and GML §103-g, the initial list is expected to be issued no later than 120 days after the Act's effective date, at which time it will be posted on the OGS website.

By submitting a response to this solicitation or by assuming the responsibility of a Contract awarded hereunder, Vendor (or any assignee) certifies that once the prohibited entities list is posted on the OGS website, it will not utilize on such Contract any subcontractor that is identified on the prohibited entities list.

Additionally, Vendor is advised that once the list is posted on the OGS website, any Vendor seeking to enter into, renew or extend a Contract or assume the responsibility of a Contract awarded in response to the solicitation, must certify at the time the Contract is bid upon or a proposal submitted, or the contract is renewed, extended or assigned that it is not included on the prohibited entities list.

During the term of the Contract, should BOCES receive information that a person is in violation of the above-referenced certification, BOCES will offer the person an opportunity to respond. If the person fails to demonstrate that it has ceased its engagement in the investment which is in violation of the Act within 90 days after the determination of such violation, then BOCES shall take such action as may be appropriate including, but not limited to, imposing sanctions, seeking compliance, recovering damages, or declaring the Vendor in default.

BOCES reserves the right to reject any bid, proposal or request for assignment for an entity that appears on the prohibited entities list prior to the award of a contract, and to pursue a responsibility review with respect to any entity that is awarded a contract and appears on the prohibited entities list after contract award.

Signature:____________________

Print Name: Marc C Fiore

Title: President

Company Name: Mindox

Date: 4/18/2020