



schooltool.com

☎ 585.424.3590

☎ 585.424.3809

250 Alexander Street
Rochester, NY 14607

DATA PROTECTION ADDENDUM

This Data Protection Addendum ("Addendum") is incorporated into and made a part of the agreement between Mindex Technologies, Inc. ("Vendor") and Washington-Saratoga-Warren-Hamilton-Essex BOCES ("Customer"), effective February 16, 2021 ("Agreement").

WHEREAS the Parties wish to update the Agreement for compliance with the requirements of New York Education Law Section 2-d ("Section 2-d");

For and in consideration of the mutual covenants and agreements contained herein, Vendor and Customer agree as follows:

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. Adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework as of July 1, 2020;
- b. Comply with Customer's data security and privacy policy and Section 2-d;
- c. Limit internal access to Personally Identifiable Information to only those employees or sub-contractors that need access to provide the services under the Agreement;
- d. Not use the Personally Identifiable Information for any purpose not explicitly authorized in the Agreement and this Addendum thereto;
- e. 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;
- f. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality, and integrity of Personally Identifiable Information in Vendor's custody;
- g. 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;
- h. Use commercially reasonable encryption to protect Personally Identifiable Information in Vendor's custody while in motion or at rest; and
- i. 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. Customer Obligations.

- a. Customer represents, warrants, and covenants to Vendor that Customer owns or otherwise has and will have the necessary rights and consents in and relating to the Personally Identifiable Information, including by presenting, complying with, and enforcing all appropriate disclosure and notice requirements at the point of collection of Personally Identifiable Information, so that, as accessed, received, and processed by Vendor in accordance with the Agreement and this Addendum thereto, it does not and will not infringe, misappropriate, or otherwise violate any intellectual property rights or any privacy or other rights of any third party or violate any applicable law, including without limitation the Family Educational Rights and Privacy Act and Section 2-d.
- b. Customer will not, and will not permit any other person to, access or use the Services except as expressly permitted by this Agreement. For purposes of clarity and without limiting the generality of the foregoing, Customer will not, and will not permit a user of the Services to, except as the Agreement expressly permits: (i) copy, modify, or create derivative works or improvements of the Services; (ii) reverse engineer, disassemble, decompile, decode, adapt, or otherwise attempt to derive or gain access to the source code of the Services, in whole or in part; bypass or breach any security device or protection used by the Services or access or use the Services other than by an Authorized User through the use of his or her own then valid Access Credentials; input, upload, transmit, or otherwise provide to or through the Services, any information or materials that are unlawful or injurious, or contain, transmit, or activate any harmful code; (vi) damage, destroy, disrupt, disable, impair, interfere with, or otherwise impede or harm in any manner the Services, Vendor systems, or Vendor's provision of services to any third party, in whole or in part; (vii) remove, delete, alter, or obscure any trademarks or other intellectual property or proprietary rights notices from any Services, including any copy thereof; (viii) access or use the Services in any manner or for any purpose that infringes, misappropriates, or otherwise violates any intellectual property right or other right of any third party, or that violates any applicable law; or (ix) access or use the Services or Vendor for purposes of competitive analysis of the Services or Vendor documentation, the development, provision, or use of a competing software service or product or any other purpose that is to the Vendor's detriment or commercial disadvantage; or (xi) otherwise access or use the Services beyond the scope of the authorization granted under the Agreement. Customer will remain solely responsible and liable for all use of the Services due to Customer's acts or omissions.

4. 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 Exhibits 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.
5. **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.

[Signature Page to Follow]

IN WITNESS WHEREOF, the parties hereto have duly executed this Addendum as of the Effective Date.

MINDEX TECHNOLOGIES, INC.

By: Marc F. Fione

Name: Marc F. Fione

Title: President

WSWHE BOCES

By: Anthony Muller

Name: Anthony Muller

Title: Deputy District Superintendent

EXHIBIT A

Parent's Bill of Rights for Data Security and Privacy Washington-Saratoga-Warren-Hamilton- Essex BOCES

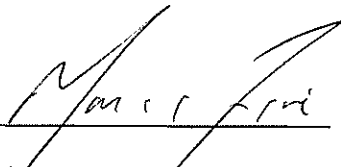
EDUCATION LAW §2-d Bill of Rights for Data Security and Privacy

The Washington-Saratoga-Warren-Hamilton-Essex BOCES is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

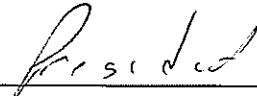
Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, 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); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available for public review at www.nysed.gov/data-privacy-security, and by writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of student data addressed.
 - o Contact WSWHE BOCES Data Protection Officer: Dr. Turina Parker, Executive Director for Educational & Support Programs, by email: tuparker@wswhiboces.org, or by phone: 518-581-3716. Complaints should be submitted in writing using the form that is available on the BOCES website and in the BOCES offices.
 - o Complaints may also be submitted to NYSED online at www.nysed.gov/data-privacy-security, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, by email to privacy@nysed.gov, or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

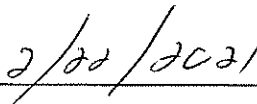
BY THE VENDOR:



Signature



Title



Date

EXHIBIT 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 Dr. Turina Parker, Assistant Superintendent for Educational & Support Programs, tuparker@wswhoboces.org or (518) 581-3716.
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. No later than July 1, 2020, the measures that Vendor will take to protect Personally Identifiable Information include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework.
 - b. **Encryption.** Vendor will encrypt data in motion and at rest using methodology in accordance with 2-d.

