SCHOOLTOOL

schooltool.com
585.424.3590
585.424.3809
250 Alexander
Street Rochester,
NY 14607

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Mindex Technologies, Inc. (the "Contractor" or "Mindex Technologies") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes

> "Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA. For the avoidance of doubt, Mindex does not collect
>
> Personally identifiable information from the records of ESBOCES and/or participating school districts relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to

comply with ESBOCES' policy(ies) on data security and privacy. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data caused by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of ESBOCES' and/or participating school districts' Protected Data in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option and direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the data security and privacy policy of ESBOCES; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. 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.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

MINDEX TECHNOLOGIES, INC.

BY: Marc Jin **DATED:** 7/21/2019

MINDEX CONFIDENTIAL: DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN. THIS DATA PRIVACY AND SECURITY PLAN IS CONFIDENTIAL AND SUBJECT TO THE CONFIDENTIALITY PROVISIONS OF THE LICENSE AGREEMENT BETWEEN THE PARTIES DATED SEPTEMBER 1, 2011.

1. **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 ESBOCES's data security and privacy policy, Contractor will:
        i. Follow policies and procedures compliant with (i) relevant state, federal, and local data security and privacy requirements, including Education Law § 2-d, (ii) this Data Security and Privacy Plan, and (iii) ESBOCES's data security and privacy policy;
        ii. Implement commercially reasonable administrative, technical, operational, and physical safeguards and practices to protect the security of Protected Data in accordance with relevant law;
        iii. Follow policies compliant with ESBOCES's Parents' Bill of Rights and the supplemental information to the agreement between Contractor and ESBOCES (the "Agreement");
        iv. Annually train its officers and employees who have access to Protected Data on relevant federal and state laws governing confidentiality of Protected Data; 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 Protected Data in accordance with relevant law.

    b. **Safeguards.** To protect Protected Data that Contractor receives under the Agreement, Contractor will follow policies that include the following administrative, operational, and technical safeguards:
        i. Contractor will identify reasonably foreseeable internal and external risks relevant to its administrative, technical, operational, and physical safeguards;
        ii. Contractor will assess the sufficiency of safeguards in place to address the identified risks;
        iii. Contractor will adjust its security program in light of business changes or new circumstances;
        iv. Contractor will regularly test and monitor the effectiveness of key controls, systems, and procedures; and
        v. Contractor will protect against the unauthorized access to or use of Protected Data.

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

    d. **Subcontractors.** Contractor will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the Agreement. In the event that Contractor 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.** Contractor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, by following an incident response policy for identifying and responding to incidents, breaches, and unauthorized disclosures. Contractor will notify ESBOCES of any breaches or unauthorized disclosures of Protected Data promptly but in no event more than seven (7) days after Contractor has discovered or been informed of the breach or unauthorized release.

f. **Effect of Termination or Expiration**. Contractor will return all of ESBOCES' and/or participating school districts' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission at such time that the Agreement is terminated or expires.

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

1. **Exclusive Purpose**. Contractor will use the Protected Data to which it is provided access for the exclusive purpose of providing Contractor's services as more fully described in the Agreement. Contractor agrees that it will not use the Protected Data 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, Contractor will obligate its subcontractors, assignees, or other authorized persons or entities to whom it discloses Protected Data 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 Contractor to such data protection obligations imposed on Contractor by state and federal laws and regulations (e.g. 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) Contractor no longer providing services to ESBOCES and (ii) termination of the Agreement in accordance with its terms.
    b. Contractor will return all of ESBOCES' and/or participating school districts' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission 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 Protected Data provided by ESBOCES to Contractor by:
    a. Inquiries or complaints should be directed to the Associate Superintendent for Curriculum at your district or in writing to: Chief Privacy Officer, New York State Education Dept., 89 Washington Avenue, Albany, NY 12234; CPO@mail.nysed.gov.

5. **Data Storage and Security Protections**.
    a. **General**. Any Protected Data that Contractor receives will be stored on systems maintained by Contractor, or by a subcontractor under the direct control of Vendor, in a secure data center facility. Contractor will maintain reasonable administrative, technical and physical safeguards in accordance with 2-d to protect the security, confidentiality, and integrity of Protected Data in Contractor's custody.
    b. **Encryption**. Contractor will encrypt data in motion and at rest using methodology in accordance with Education Law § 2-d.