BDI-3 / easy CBM RTA

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

EDUTECH

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES/EduTech) and Riverside Assessments, LLC **("Vendor")** are parties to a contract dated February 1, 202 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, the BDI-3 Assessment ("Product"). Wayne-Finger Lakes BOCES/EduTech use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1. "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from BOCES or is created by the Vendor's product or service in the course of being used by BOCES.

2.2. "Vendor" means Riverside Assessments, LLC dba Riverside Insights.

2.3. "Educational Agency" means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES/EduTech.

2.4. "BOCES" means the Wayne-Finger Lakes BOCES/EduTech.

2.5. "Parent" means a parent, legal guardian, or person in parental relation to a Student.

2.6. "Student" means any person attending or seeking to enroll in an educational agency.

2.7. "Eligible Student" means a student eighteen years or older.

2.8. "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.9. "This Contract" means the underlying contract as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

5. Vendor EmployeeTraining

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from BOCES or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. Ownership and Location of Protected Information

7.1. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with BOCES. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2. BOCES shall have access to the BOCES's Protected Information at all times through the term of this Contract. BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

7.3. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users, or performing any other data analytics other than those required to provide the Product to BOCES. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.

7.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. Purpose for Sharing Protected Information

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to Wayne-Finger Lakes BOCES/EduTech.

9. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

10. Protected Information and Contract Termination

10.1. The expiration date of this Contract is defined by the underlying contract.

10.2. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.

10.3. Vendor shall upon BOCES' written request thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities, subject to Vendor's backup retention policies and except as required by applicable law, regulation, court order, subpoena, or similar legal process.

10.5. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10.6. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2. Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

12.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

12.3. align with the NIST Cybersecurity Framework 1.0;

12.4. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

12.5. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (Attachment B);

12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

12.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

12.8. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

12.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

12.10. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and

12.11. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated orexpires.

13. Additional VendorResponsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse BOCES for the full cost incurred by BOCES to send notifications required by Education Law Section 2-d.

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Signatures

For Wayne-Finger Lakes BOCES/EduTech	**For (Vendor Name)**
	Riverside Assessments, LLC dba Riverside Insigh
Date 2/20/24	**Date** February 14, 2024

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment A – Parent Bill of Rights for Data Security and Privacy

Wayne-Finger Lakes BOCES (EduTech)

Parents' Bill of Rights for Data Privacy and Security

The Wayne-Finger Lakes BOCES (EduTech)seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our BOCES and school operations.

The Wayne-Finger Lakes BOCES (EduTech)seeks to insure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the Wayne-Finger Lakes BOCES (EduTech) has posted this Parents' Bill of Rights for Data Privacy and Security.

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. The procedures for exercising this right can be found in Board Policy 5500 entitled Family Educational Rights and Privacy Act (FERPA).
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 at http://www.nysed.gov/data-privacy-security/student-data-inventory and a copy may be obtained 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 the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Revised October 2019

Signatures

For Wayne-Finger Lakes BOCES/EduTech	Scott E. Olson **For (Vendor Name)**
	Riverside Assessments, LLC dba River:
Date	**Date**
2/20/24	February 14, 2024

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment B – Wayne-Finger Lakes BOCES/EduTech Data Privacy and Security Policy

In accordance with New York State Education Law §2-d, the BOCES hereby implements the requirements of Commissioner's regulations (8 NYCRR §121) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or "NIST CSF").

In this regard, every use and disclosure of personally identifiable information (PII) by the BOCES will benefit students and the BOCES (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

The BOCES also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the BOCES will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see Policy 6320 and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the BOCES will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The BOCES will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

The Board of Education values the protection of private information of individuals in accordance with applicable law and regulations. Further, the BOCES Director of Educational Technology is required to notify parents, eligible students, teachers and principals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy and New York State Education Law §2-d

a) "Private information" shall mean **personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number.
2. Driver's license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password, which would permit access to an individual's financial account.
4. Any additional data as it relates to administrator or teacher evaluation (APPR)

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

**"Personal information" shall mean any information concerning a person, which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b) Personally Identifiable Information, as applied to student data, means 40 personally identifiable information as defined in section 99.3 of Title 34 of the Code of 41 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 42 U.S.C 1232-g, and as applied to teacher and principal data, means personally 43 identifying information as such term is defined in Education Law §3012-c(10).

c) Breach means the unauthorized access, use, or disclosure of student data 9 and/or teacher or principal data. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Notification Requirements
Methods of Notification

The required notice shall be directly provided to the affected persons and/or their guardians by one of the following methods:

a) Written notice;

b) Secure electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the BOCES when notifying affected persons in electronic form. However, in no case shall the BOCES require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying BOCES and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired. This notice shall take place 60 days of the initial discovery.

In the event that any residents are to be notified, the BOCES shall notify the New York State Chief Privacy Officer, the New York State Cyber Incident Response Team, the office of Homeland Security, and New York State Chief Security Officer as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected residents.
The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR §121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

Data Protection Officer

The BOCES has designated a BOCES employee to serve as the BOCES's Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the BOCES.

The BOCES will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Annual Data Privacy and Security Training

The BOCES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations.

References:

Education Law §2-d

8 NYCRR §121

Family Educational Rights and Privacy Act of 1974, 20 USC §1232(g), 34 CFR 99

Individuals with Disabilities Education Act (IDEA), 20 USC §1400 et seq., 34 CFR 300.610–300.627

Attachment C – Vendor's Data Security and Privacy Plan

The Wayne-Finger Lakes BOCES Parents Bill of Rights for Data Privacy and Security, which is included as Attachment B to this Addendum, is incorporated into and make a part of this Data Security and Privacy Plan.

(Vendor can attach)

Riverside Insights
Education Law §2-d, Part 121 Compliance

Chapter 56 of the Laws of 2014 added §2-d to the Education Law as of April 2014 ("Education Law 2-d"). Education Law 2-d outlines certain requirements for educational agencies and their third-party contractors to ensure the security and privacy of protected information. Part 121 of the Commissioner's regulations promulgated under Education Law 2-d ("Part 121"), among other things, clarifies the data security and privacy obligations of educational agencies and third-party contractors, establishes requirements for contracts and other written agreements where personally identifiable information ("PII") will be provided to a third-party contractor, and establishes the National Institute of Standards and Technology ("NIST") Cybersecurity Framework as the standard for educational agencies data security and privacy programs.

As a third-party contractor that processes student data from educational agencies in New York State, Riverside Assessments, LLC dba Riverside Insights ("Riverside") is subject to the requirements of Education Law 2-d, including Part 121. This Attestation describes the requirements of Part 121, Section 121.9(a), which applies to all third-party contractors who receive student data from educational agencies in New York State, and explains how Riverside satisfies these requirements.

7 Principles Governing Third-Party Contractors under Education Law 2-d

1. ***Adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework; comply with the data security and privacy policy of the educational agency with whom it contracts.***

   Riverside uses SQL TDE encryption (AES-256) for data at rest and SSL/TLS 1.2 (2048-bit) for data in transit. Riverside encryption processes for data at rest and in transit are consistent with NIST Special Publication 800-111 and successor publications. Riverside's encryption processes for data in transit comply with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; 800-113, Guide to SSL VPNs; and others processes validated under the Federal Information Processing Standards ("FIPS") 140-2.

   Usernames, passwords, and any other means of gaining access to our platforms or to Student Data, are managed by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3.

   Riverside's data center providers have formally documented incident response plans addressing the purpose, scope, roles, responsibilities, and management commitments of its personnel. The providers developed these commitments align with ISO 27001 and NIST 800-53 standards.

2. ***Limit access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services.***

   Internal Riverside employees and subcontractors do not as a matter of course have viewable access to personally identifiable information. Our entitlement process is documented and is triggered by our Human Resources system for management by our IT support team. Riverside

performs user access reviews on a quarterly basis and works with business managers to verify user entitlements.

All user account requests are submitted via our internal ticketing system. Depending on what account(s) or access is requested, the requests are processed by our Technical Assistance Center ("TAC") or customer operations ("Customer Ops") teams. New accounts or access permissions require approval from the Riverside employee's/contractor's manager and are provisioned based on the "principle of least privilege," which means that the minimum access and functionality necessary to perform an operation should be granted and only for the minimum amount of time necessary.

The entitlements for our external product systems are managed directly by the client's account administrator. The applications have role and permissions models that can be managed and edited as needed to meet the specific business needs. Riverside does not access or manage these systems for clients unless needed as part of a technical support effort where access to customer data is permissioned at the point of contact. This process is documented in the user guides provided to administrators at the time of set up and is accessible within the help platform in the product.

Access to the information is monitored and controlled using several "defense in depth" techniques, including role-based access control, AWS security groups and ACLs, and firewalls.

Further, when a Riverside employee leaves the company or Riverside ends its engagement with a sub-contractor, managers will provide notice to the TAC and Customer Ops teams so that access can de-provisioned to the affected systems as soon as possible, but no later than within 24 hours.

3. ***Not use the personally identifiable information for any purpose not explicitly authorized in its contract.***

Riverside only uses PII for the purposes of delivering and improving the services it provides to customers authorized under a contract. Riverside codified this commitment in its Privacy Policies, which Riverside reviews and updates annually, and implements through the processes and tools described below.

Riverside's documented policies prohibit personnel, including subcontractors, from releasing any information to anyone outside of Riverside, regardless of medium (e.g., voice, email, film, tape, document) and pertaining to any part of a contract, project, or program, unless doing so is required in order to deliver services to customers, the customer otherwise consents to such disclosure, the information is in the public domain before the date of release, or the disclosure is required under applicable law or court order. Riverside also has policies governing transportable devices that mitigates the risk of PII being removed outside its permissible environment.

To monitor and enforce the policies above, Riverside implements, among other things, the access controls described in Section 2 and logs and audit records.

Riverside's access controls, including its use of the "principle of least privilege," are designed to mitigate the risk of individuals accessing PII when they do not have a basis for doing so per Riverside's contractual obligations.

Asset custodians are required to implement auditing of systems and applications that link access to system components to individual users. In addition, Riverside retains access records and logs for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. For critical or sensitive systems:

- Log entries must be immediately available for a minimum of 90 days (online);
- Log entries must be available for 365 days (online or offline storage); and
- Logs must be exportable or transferable in an automated fashion.

Riverside retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes.

Finally, Riverside has policies to lock down transportable devices such as USB drives, removable media, etc., through the Group Policy feature of Microsoft's Active Directory. Devices are regularly monitored when on the network.

4. ***Except for authorized representatives of the third-party contractor 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, not disclose any personally identifiable information to any other party: (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides 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.***

As described in more detail in Sections 2 and 3, Riverside implements tools and processes designed to prevent the disclosure of PII to other parties, except for those authorized to access such PII under Riverside's contract with its customers to the extent needed for Riverside to deliver its services or under the exceptions described in Section 3. Riverside employs a documented entitlement process, and new accounts and access privileges are allocated based on the "principle of least privilege."

Moreover, Riverside has written contracts with its third-party service providers that address the providers' responsibilities, including confidentiality and notification obligations in the event of a security incident or breach.

5. ***Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody as prescribed by state and federal law, regulations and its contract with the educational agency.***

- *Administrative Safeguards*: Role-Based Access Control ("RBAC") enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities through requiring access

enforcement that (i) assigns privileges to individuals based on job classification and function, (ii) restricts access based on a user's need to know, and (iii) is set to "deny all" unless specifically allowed. Personnel annually complete mandatory computer-based data security and privacy training hosted through a third-party research ethics and compliance training organization, with assessments at the end of the training to verify comprehension. Riverside also includes practical exercises in this security awareness training that simulate actual cyber-attacks. Some of these exercises cover no-notice social engineering activities.

- *Technical Safeguards*: Riverside engages a third-party vendor to perform annual penetration testing on our application systems. This testing involves a battery of attacks against customer-facing websites, and the vendor provides detailed reporting at the conclusion of testing. Riverside promptly remediates any vulnerabilities identified in this testing according to the level of severity. PII is encrypted both at rest and in transit (see Section 6 for more details). All information stored on Riverside's systems is protected with file system, network share, claims, application, or database specific access control lists. Riverside uses email gateway products to centrally manage spam protection mechanisms, including signature definitions, in order to reduce the introduction of malicious software to client systems. Email messages and attachments are also encrypted. The email gateway product prevents the delivery of potentially dangerous messages to riverside users and quarantines them for manual inspection. Notifications of malicious messages and/or attachments are sent to the TAC team for investigation and, if necessary, the mitigation of any potential threats.

- *Physical Safeguards*: The production facilities for US-based customers are maintained by third-party hosts' data centers that are all SSAE16 SOC 2 Type 2 audited hosting centers The production systems computer rooms at these facilities are designed from the ground up to minimize risk of power and climate control failure. All our hosting providers perform periodic testing and auditing of their facilities. All facilities have full battery and generator power, so in case of an outage, power is maintained indefinitely. All production systems are fully protected by UPS systems and emergency power generators. Riverside has written contracts with its third-party hosting providers that address the providers' notification obligations in the event of a security incident or breach at the data center. With respect to Riverside's facilities, Riverside's main office and off-site scoring center are protected by an intrusion detection alarm system that is monitored from a central location. In addition, both facilities are assigned a 24/7 security guard. Riverside's facilities are protected by smoke and fire detection alarm systems located throughout each facility.

6. ***Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using controls as specified 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.***

Riverside protect data in accordance with Section 13402(h)(2) of Public Law 111-5 by encrypting data both at rest and in transit. Riverside's encryption methods follow FIPS 140-2 validated encryption technologies. Customer data is stored in a secure data center in the continental United States and is encrypted with industry-standard high-security encryption. For both web and mobile we use SQL TDE encryption (AES-256) for data at rest and SSL/TLS 1.2 (2048-bit) for data in transit.

7. ***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.***

Riverside only processes PII for the purposes of delivering and improving the Services it provides to its customers pursuant to its written agreements with them. As described in Riverside's Privacy Policies, Riverside does not sell, use, or disclose PII for any marketing or commercial purpose or facilitate any such sale, use, or disclosure by any other party. The administrative, technical, and physical safeguards described in this Attestation are designed to monitor and enforce Riverside's prohibitions against unauthorized use of PII.

Addendum B

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE**: The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by Riverside Assessments, LLC dba Riverside Insights (the "Contractor") are limited to the purposes authorized in the contract between the Contractor and the Wayne-Finger Lakes BOCES/EduTech (the "BOCES") dated February 1, 2024 (the "Contract").

2. **SUBCONTRACTOR OVERSIGHT DETAILS**: The Contractor will ensure that any subcontractors, or other authorized persons or entities to whom the Contractor will disclose the Confidential Data, if any, are contractually required 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 (e.g., the Family Educational Rights and Privacy Act ("FERPA"); Education Law §2-d; 8 NYCRR Part 121).

3. **CONTRACT PRACTICES**: The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the BOCES in CSV or similar format and/or destroyed by the Contractor as directed by the BOCES.

4. **DATA ACCURACY/CORRECTION PRACTICES**: A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in FERPA, stored by the BOCES in a Contractor's product and/or service by following the BOCES' procedure for requesting the amendment of education records under FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by the BOCES in Contractor's product and/or service by following the appeal procedure in the BOCES' APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

5. **SECURITY PRACTICES**: Confidential Data provided to Contractor by the BOCES will be stored in the United States. The measures that Contractor takes to protect Confidential Data will align with the NIST Cybersecurity Framework including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

6. **ENCRYPTION PRACTICES**: The Contractor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Signature: Scott E. Olson

Date: February 14, 2024