RIDER

This is a Rider to the contract (including any terms of services or terms of use or any other policies, terms, agreements, or understandings referenced therein) between the Commack Union Free School District ("the District") and Riverside Assessments, LLC ("the Contractor"), that is being entered for a term from 4/12/24 through 6/30/27 for use of CogAT pursuant to the attached quote ("the Contract")(collectively, the Contract and Rider are referred to as "the Agreement").

To the extent that the provisions of this Rider and the annexed Data Privacy Agreement are inconsistent with any terms set forth in the Contract, the provisions of this Rider and the annexed Data Privacy Agreement will control.

1. Plan for Security and Protection of Personally Identifiable Information

   A. "District Data" means all information obtained by the Contractor from the District or by the Contractor in connection with the Services provided by the Contractor pursuant to this Agreement, including but not limited to business, administrative and financial data, intellectual property, student and personnel data, and metadata. The term, "District Data" does not include any information made publicly available by the District, except PII from student and personnel data which will be considered "District Data" regardless of whether or not it is made public.

   B. "Personally Identifiable Information" or "PII" includes, but is not limited to: (i) a person's name or address or the names or addresses of a student's parents or other family members; (ii) any personal identifier (e.g., SSN, student number or biometric record); (iii) indirect identifiers (e.g., date of birth, place of birth, or mother's maiden name); (iv) other information that alone or in combination is linked or linkable to a specific individual and would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances to identify the individual with reasonable certainty; and (v) any information requested by a person who the District or Contractor reasonably believes knows the identity of the person to whom a record relates.

   C. The Contractor represents and warrants that it will comply with all District policies and State, federal and local laws, regulations, rules and requirements related to the confidentiality, security and privacy of District Data.

   D. The Contractor represents and warrants that District Data received by the Contractor will be used only to perform Contractor's obligations pursuant to the Agreement and for no other purpose; provided, de-identified District Data may be used for the purposes set forth in Section 14 of the attached Terms of Use.

E. The Contractor represents and warrants that it will only collect data from the District or District employees or other End Users (the term "End Users" means the individuals authorized by the District to access and use services provided by the Contractor pursuant to the Agreement) that is necessary to fulfill the Contractor's duties pursuant to the Agreement.

F. The Parties agree that all rights including all intellectual property rights in and to District Data will remain the exclusive property of the District and that the Contractor has a limited, non-exclusive license to use District Data solely to perform the Services pursuant to the Agreement.

G. If the Contractor has access to District Data that is subject to the Family Educational Rights and Privacy Act ("FERPA"), the Contractor acknowledges that for purposes of the Agreement it will be designated as a "school official" with a "legitimate educational interest" pursuant to FERPA and its implementing regulations, and the Contractor agrees to abide by the limitations and requirements imposed on school officials.

H. The Contractor must execute and deliver the Data Privacy Agreement annexed hereto as Exhibit A simultaneously with the execution and delivery of this Rider. The terms of the Data Privacy Agreement are hereby incorporated into this Rider.

I. All the provisions of this Paragraph will survive the expiration or sooner termination of the Agreement.

2. Indemnification by the District: If the Contract has any provision that requires the District to indemnify, defend and/or hold harmless the Contractor, such provision will be void and have no force or effect.

3. Entire Agreement/No End User Agreements: The Agreement contains the entire agreement of the parties with respect to the subject matter thereof and supersedes any and all other agreements, understandings and representations, written or oral, by and between the parties. In the event that any part of the Agreement references terms of service or terms of use or any other policies, terms, agreements or understandings, the applicable policies, terms, agreements or understandings are those that were in effect on the date of the Contract, unless the applicable policies, terms, agreements or understandings were modified pursuant to Paragraph 6 of this Rider. In the event that the Consultant requires District employees or other End Users to enter into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, those agreements and/or understandings will be null, void and without effect, except for the Terms of Use attached hereto, and the terms of the Agreement will apply.

4. Termination: The Agreement may be terminated by the District immediately upon the Contractor's breach of the Contractor's obligations set forth in paragraph 1 of this Rider. Upon termination of the Agreement, the Contractor is not entitled to any further payments hereunder.

5. Notices: Any notices required or permitted to be given pursuant to the terms of the Agreement must be in writing and either personally delivered or sent by nationally recognized overnight carrier to the parties at the following addresses:

To the Contractor:

Riverside Insights
One Pierce Place, Suite 101C
Itasca, IL 60143
Attn: General Counsel

To the District:
Commack Union Free School District
PO Box 150
Commack, NY 11725
Attention: Superintendent of Schools

With a copy to:
Bond, Schoeneck & King
225 Old Country Road
Melville, New York 11746
Attention: Eugene R. Barnosky, Esq.

If the notice is sent by personal mail, it will be deemed delivered upon receipt and if sent by registered or certified mail, it shall be deemed delivered 3 days after so mailing.

6. Modification: The Agreement may not be changed by any District Employee or other End User. The Agreement may not be changed orally, electronically, by click-through agreement, or by continued use. The Agreement may only be changed by an agreement in writing signed by the District. Any waiver of any term, condition or provision of the Agreement will not constitute a waiver of any other term, condition or provision, nor will a waiver of any breach of any term, condition or provision constitute a waiver of any subsequent or succeeding breach.

7. Governing Law, Choice of Forum and Waiver of Jury Trial: The Agreement is subject to, governed by, enforced according to and construed according to the laws of the State of New York, without regard to the conflicts of laws provisions thereof. Notwithstanding the arbitration provisions in the Contract, if any, the parties agree that any dispute arising under the Agreement will be litigated in a New York State Court in Suffolk County, New York. The parties each waive trial by jury in any action concerning the Agreement.

8. No Assignment: In accordance with the provisions of New York General Municipal Law § 109, the Contractor is hereby prohibited from assigning, transferring, conveying, subletting or otherwise disposing of the Agreement, or of the Contractor's rights, title, or interest in the Agreement, or the Contractor's power to execute the Agreement to any other person or corporation without the previous consent in writing from the District.

9. Third-Party Beneficiaries: There are no third-party beneficiaries in the Agreement.

10. Execution: This Rider may be executed in one or more counterparts, all of which

shall be considered one and the same agreement. This Rider may be executed by facsimile or PDF signature, each of which shall constitute an original for all purposes.

11. Notwithstanding the execution of this Rider or any other term or condition of this Rider, it will not become effective unless and until the Contract between the parties is in full force and effect.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement.

Commack Union Free School District

By: _____
Alise Pulliam
Executive Director for Instructional Technology

Riverside Assessments, LLC
dba Riverside Insights **, the Contractor**

By: Scott E. Olson
Name: Scott E. Olson
Title: Manager of Proposal Services

EXHIBIT A

DATA PRIVACY AGREEMENT

COMMACK UNION FREE SCHOOL DISTRICT
DATA PRIVACY AGREEMENT

Between

COMMACK UNION FREE SCHOOL DISTRICT

and

This Data Privacy Agreement ("DPA") is by and between the Commack Union Free School District ("the District") and ("the Contractor"), collectively, "the Parties."

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms have the following meanings:

1. Breach: The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information of District Data, or a breach of the Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.

2. Commercial or Marketing Purpose: The sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.

3. Disclose: To permit access to, or the release, transfer, or other communication of Personally Identifiable Information by any means, including oral, written or electronic, whether intended or unintended.

4. District Data: All information obtained by the Contractor from the District or by the Contractor in connection with the Services provided by the Contractor pursuant to the Service Agreement, including but not limited to business, administrative and financial data, intellectual property, student and personnel data, and metadata. The term, "District Data" does not include any information made publicly available by the District, except Personally Identifiable Information from student and personnel data which will be considered "District Data" regardless of whether or not it is made public.

5. Education Record: An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

6. Educational Agency: As defined in Education Law 2-d, a school district, board of cooperative educational services, School, or the New York State Education Department.

7. Eligible Student: A student who is eighteen years of age or older.

8. Encrypt or Encryption: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR § 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

9. NIST Cybersecurity Framework: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

10. Parent: A parent, legal guardian or person in parental relation to the Student.

11. Personally, Identifiable Information ("PII"): Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.

12. Release: Has the same meaning as Disclose.

13. Service Agreement:

The attached Terms of Use.

14. Services: The services provided by the Contractor to the District pursuant to the Service Agreement.

15. School: Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.

16. Student: Any person attending or seeking to enroll in an Educational Agency.

17. Student Data: Personally, Identifiable Information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g. Personally Identifiable Information includes, but is not limited to: (i) a person's name or address or the names or addresses of a Student's parents or other family members; (ii) any personal identifier (*e.g.*, SSN, student number or biometric record); (iii) indirect identifiers (*e.g.*, date of birth, place of birth, or mother's maiden name); (iv) other information that alone or in combination is linked or linkable to a specific individual and would allow a reasonable person in the District community who does not have personal knowledge of the relevant circumstances to identify the individual with reasonable certainty; and (v) any information requested by a person who the District or the Contractor reasonably believes know the identity of the person to whom a record relates.

18. Subcontractor: The Contractor's non-employee agents, consultants and/or other persons or entities not employed by the Contractor who are engaged in the provision of Services pursuant to the Service Agreement.

19. Teacher or Principal APPR Data: Personally, Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to Release pursuant to the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for the Contractor to provide Services to the District pursuant to the Service Agreement; the Contractor may receive District Data regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C.§§ 6501-6506 (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); New York Education Law § 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law and to protect District Data. The Contractor agrees to maintain the confidentiality and security of District Data in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

The Contractor has no property or licensing rights or claims of ownership to District Data, and the Contractor must not use District Data for any purpose other than to provide the Services set forth in the Service Agreement. The Contractor agrees that neither the Services provided to the District nor the manner in which the Services are provided by the Contractor will violate applicable New York, federal and local laws, rules and regulations.

If the Contractor has access to District Data that is subject to the Family Educational Rights and Privacy Act ("FERPA"), the Contractor acknowledges that for purposes of this Agreement it will be designated as a "school official" with a "legitimate educational interest" pursuant to FERPA and its implementing regulations, and the Consultant agrees to abide by the limitations and requirements imposed on school officials.

3. Collection of Data.

The Contractor represents and warrants that it will only collect data from the District or District employees or other End Users (the term "End Users" means the individuals authorized by the District to access and use the Services) that is necessary to fulfill the Contractor's duties pursuant to the Service Agreement.

4. Data Security and Privacy Plan.

The Contractor must adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect District Data in a manner that complies with New York, federal and local laws, rules and regulations and the District's policies. Education Law § 2-d requires that the Contractor provide the District with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable State, federal and local data security and privacy requirements. The Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C and is incorporated into this DPA.

5. The District's Data Security and Privacy Policy

State law and regulation requires the District to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. The Contractor represents and warrants that it will comply with the District's data security and privacy policy and other applicable policies.

6. Right of Review and Audit.

Upon request by the District, the Contractor will provide the District with copies of its policies and related procedures that pertain to the protection of PII and District Data. The policies and procedures may be made available in a manner that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required by the District to undergo an audit of Contractor's privacy and security safeguards, measures and controls as they pertain to alignment with the requirements of applicable New York, federal and local laws, rules and regulations, the District policies applicable to the Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at the Contractor's expense, and provide the written audit report to the District. The Contractor may provide the District with a recent industry standard audit report performed by an independent third party on the Contractor's privacy and security practices as an alternative to undergoing an audit. The determination of whether the previously prepared audit report is "recent" will be determined by the District in its sole judgment.

7. Access to/Disclosure of District Data

(a) The Contractor agrees that it will limit the Contractor's internal access to and only Disclose PII to the Contractor's officers, employees and Subcontractors who need to access the PII in order to provide the Services and that the disclosure of PII will be limited to the extent necessary to provide the Services pursuant to the Service Agreement. The Contractor must take all actions necessary to ensure that all its officers, employees and Subcontractors comply with the terms of this DPA.

(b) The Contractor must ensure that each Subcontractor performing functions pursuant to the Service Agreement where the Subcontractor will receive or have access to District Data must be contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

(c) The Contractor must examine the data security and privacy measures of its Subcontractors prior to utilizing the Subcontractor to ensure compliance with this DPA. If at any point a Subcontractor fails to materially comply with the requirements of this DPA, the Contractor must: notify the District and prevent the Subcontractor's continued access to District Data; and, as applicable, retrieve all District Data received or stored by Subcontractor and/or ensure that District Data has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the Subcontractor compromises PII, the Contractor must follow the Data Breach reporting requirements set forth herein.

(d) The Contractor will take full responsibility for the acts and omissions of its officers, employees and Subcontractors.

(e) The Contractor must not Disclose District Data to any other party (a party other than the Contractor's officers or employees or Subcontractors who does not need access to the District Data to provide the Services pursuant to the Service Agreement) without the prior written consent of the District (if necessary, the District will obtain the required consent(s) from third parties) unless the disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the District of the court order or subpoena in advance of compliance but in any case, provides notice to the District no later than the time the District Data is disclosed, unless such disclosure to the District is expressly prohibited by the statute, court order or subpoena.

(f) Except as prohibited by law, the Contractor will: (i) immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by the Contractor seeking District Data; (ii) consult with the District regarding the Contractor's response; (iii) cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and (iv) upon the District's request, provide the District with a copy of the Contractor's response.

(g) Upon the District's request, the Contractor agrees that it will promptly make any District Data held by the Contractor available to the District.

8. Training.

The Contactor must ensure that all its officers, employees and Subcontractors who have access to PII have received or will receive training on the federal and State laws governing confidentiality of the data prior to receiving access.

9. Term and Termination.

This DPA will be effective as of the date the Service Agreement is effective and will terminate on the termination of the Service Agreement. However, the obligations of the parties pursuant to this DPA will survive the expiration of the Service Agreement and will continue until the Contractor and Subcontractors no longer retain PII and no longer retain access to PII.

10. Data Return and Destruction of Data.

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the District, and the Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the District, unless such retention is expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, expressly requested by the District for purposes of facilitating the transfer of PII to the District or expressly required by law. As applicable, upon expiration or termination of

the Service Agreement, the Contractor will transfer PII, in a format agreed to by the Parties to the District.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the District's written election to do so, the Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by the Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, or electronic imaging of hard copies) as well as any and all PII maintained on behalf of the Contractor in a secure data center and/or in cloud-based facilities that remain in the possession of the Contractor or its Subcontractors, the Contractor will ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed; provided, copies of PII maintained as backups will be retained in accordance with Contractor's backup retention policies. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c) The Contractor will provide the District with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) To the extent that the Contractor and/or its Subcontractors continue to be in possession of any de-identified data (*i.e.*, data that has had all direct and indirect identifiers removed), the Contractor agrees not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

11. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or Disclose PII for a Commercial or Marketing Purpose.

12. Encryption.

The Contractor will use industry standard security measures including Encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must Encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

13. Storage.

Contractor must store all District Data within the United States of America.

14. Breach.

a. The Contractor must promptly notify the District of any Breach of PII in the most expedient way possible and without unreasonable delay and in no event more than seven calendar days after discovery of the Breach. Notifications required pursuant to this section must be in writing and by email (if email address is provided) and personal delivery or nationally recognized overnight carrier. Notifications must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for

representatives who can assist the District. Violations of the requirement to notify the District are subject to civil penalty(ies) pursuant to Education Law § 2-d. The Breach of certain PII protected by Education Law §2-d may subject the Contractor to additional penalties.

b. Notifications required to be made to the District pursuant to this paragraph must be sent to the following people at the following addresses:

Dr. Jordan Cox
Superintendent of Schools
Commack Union Free School District
PO Box 150
Commack, NY 11725
Email: jcox@commack.k12.ny.us

Mrs. Alise Pulliam
Executive Director for Instructional Technology
Commack Union Free School District
PO Box 150
Commack, NY 11725
Email: apulliam@commack.k12.ny.us

15. Cooperation with Investigations.

Contractor agrees that it will cooperate with the District and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' officers, employees or Subcontractors, as related to such investigations, will be the sole responsibility of the Contractor if the Breach is attributable to Contractor or its Subcontractors.

16. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor will pay for or promptly reimburse the District for the full cost of the District's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law § 2-d and 8 NYCRR Part 121.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law § 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the District. To the extent Student Data is held by the Contractor pursuant to the Service Agreement, the Contractor must respond within 20 calendar days to the District's requests for access to Student Data so the District can facilitate review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by the Contractor pursuant to the Service Agreement, the Contractor must promptly notify the District and refer the Parent or Eligible Student to the District.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law § 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are annexed hereto as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. The Contractor must complete and sign Exhibits A and B. Pursuant to Education Law § 2-d, the District is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA will govern and prevail, will survive the termination of the Service Agreement in the manner set forth herein, and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which will be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto will be and constitute an original signature, as if all parties had executed a single original document.

Commack Union Free School District	
By: (Signature)	By: (Signature) Scott E. Olson
Alise Pulliam	(Printed Name) Scott E. Olson
Executive Director for Instructional Technology	(Title) Manager of Proposal Services
Date: 4/15/2024	Date: April 12, 2024

CONTRACTOR'S TOTAL AGGREGATE LIABILITY FOR LOSSES OR DAMAGES RELATING TO THE AGREEMENT, REGARDLESS OF THE FORM OF ACTION, WILL IN NO EVENT EXCEED THE GREATER OF: (A) TEN THOUSAND U.S. DOLLARS (USD $10,000.00) OR (B) TWO TIMES (2X) THE FEES ACTUALLY PAID BY THE DISTRICT TO CONTRACTOR IN THE 12 MONTHS PRECEDING THE EVENT GIVING RISE TO THE LIABILITY.

IN NO EVENT WILL CONTRACTOR BE LIABLE TO THE DISTRICT OR ANY THIRD PARTY, EITHER IN CONTRACT, TORT, OR OTHERWISE, FOR ANY INDIRECT, SPECIAL, PUNITIVE, ENHANCED, EXEMPLARY, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF FUTURE REVENUE, INCOME OR PROFITS, LOSS OF DATA, OR DIMINUTION IN VALUE, ARISING OUT OF OR RELATING TO THE DISTRICT'S USE OF THE SERVICES OR IN CONNECTION WITH ANY BREACH OF THE AGREEMENT, REGARDLESS OF (X) WHETHER SUCH DAMAGES WERE FORESEEABLE, (Y) WHETHER CONTRACTOR WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND (Z) THE LEGAL OR EQUITABLE THEORY (CONTRACT, TORT, OR OTHERWISE) UPON WHICH THE CLAIM IS BASED.

THE LIMITATIONS SPECIFIED ABOVE WILL SURVIVE AND APPLY EVEN IF ANY LIMITED REMEDY SPECIFIED IN THE AGREEMENT IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

EXHIBIT A - Education Law § 2-d Parents' Bill of Rights for Data Privacy and Security

COMMACK UNION FREE SCHOOL DISTRICT

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY –

Summary of Rights and Information for Parents and Students

The legislature and governor passed a group of bills that adjusted the Regents Education Reform Agenda. These bills are known collectively as the "Common Core Implementation Reform Act." One of the key components of this act (Chapter 56, Part AA, Subpart L, of the laws of 2014) directs the Commissioner of Education to appoint a Chief Privacy Officer (CPO). A major function of this new position is to work with school districts and parents to develop elements for a parents' bill of rights to help ensure that student data is private and secure. The State Education Department (SED) and the CPO must also recommend regulations to establish standards for data security and privacy policies that will be implemented statewide.

SED has issued a preliminary Parents' Bill of Rights for Data Privacy and Security. The Commack Union Free School District is issuing this summary of parents' rights under the new law. While some additional elements will be developed in conjunction with the CPO, districts, parents and the Board of Regents, this summary sets forth the key rights and information that parents should be aware of in regards to ensuring the privacy and security of their student's educational data.

The Commack Union Free School District is committed to ensuring student privacy and recognizes that parents, legal guardians, and persons with a parental relationship to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law §2-d. To this end, the District is providing the following Parent's 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;

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 at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx or by

writing to the Office of Information & Reporting Services, New York State Education Department, Room 863, 89 Washington Avenue, New York 12234; and

5. Parents and guardians have the right to have complaints about possible breaches of student data addressed. Complaints should be addressed to Alise Pulliam, Executive Director for Instructional Technology, PO Box 150, Commack, New York 11725, Phone: (631) 912-2027, Email: alisepulliam@commack.k12.ny.us or Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.

If the Commack Union Free School District enters into a third-party contract in which the service provider receives student data or teacher or principal data in order to provide a needed service for the District, supplemental information shall be developed and provided to parents that states:

6. The exclusive purposes for which the student data or teacher or principal date will be used;

7. How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

8. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

9. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

10. Where the student data or teacher or principal data will be stored and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

The CPO as appointed by the Commissioner must secure input from parents and other education and expert stakeholders to develop additional elements for the Parents' Bill of Rights for Data Privacy and Security. The Commissioner of Education will also be promulgating regulations with a comment period for parents and other members of the public to submit comments and suggestions to the CPO.

In the meantime, you can access additional information and a question and answer document issued by SED as a preliminary Parents' Bill of Rights for Data Privacy and Security.

If you have any further questions or concerns at this time, please contact Dr. Jordan Cox, Superintendent, Commack UFSD, PO Box 150, Commack, New York 11725 or Mrs. Alise Pulliam at apulliam@commack.k12.ny.us

By: (Signature) Scott E. Olson
(Printed Name) Scott E. Olson
(Title) Manager of Proposal Services
Date: April 12, 2024

EXHIBIT B: BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and 8 NYCRR § 121.3, the District is required to post information to its website about its contracts with third-party contractors ("Service Agreements") that will receive Personally Identifiable Information ("PII") from Student Data or Teacher or Principal APPR Data.

Term of Service Agreement	Agreement Start Date: 4/12/2024 Agreement End Date: 6/30/2027
Description of the purpose(s) for which Contractor will receive/access/use PII	PII received by the Contractor will be received, accessed and used only to perform the Contractor's Services pursuant to the Service Agreement with the District. List Purposes: The exclusive purpose for which student data will be used by Service Provider is for the administration, scoring, and reporting of student assessments.
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☒ Teacher or Principal APPR Data
Subcontractor Written Agreement Requirement	The Contractor will only share PII with entities or persons authorized by the Service Agreement. The Contractor will not utilize Subcontractors without written contracts that require the Subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Service Agreement. Check applicable option. ☒ Contractor will not utilize Subcontractors.

	☐ Contractor will utilize Subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Service Agreement, the Contractor will, as directed by the District in writing: • Securely transfer data to District, or a successor contractor at the District's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data by taking actions that render data written on physical (e.g., hard copy) or electronic media unrecoverable by both ordinary and extraordinary means.
Challenges to Data Accuracy	Parents, students, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the District. If a correction to data is deemed necessary, the District will notify the Contractor. The Contractor agrees to facilitate such corrections within 21 calendar days of receiving the District's written request.
Secure Storage and Data Security	The Contractor will store and process District Data in compliance with § 2-d(5) and applicable regulations of the Commissioner of Education, as the same may be amended from time to time, and in accordance with commercial best practices, including appropriate administrative, physical and technical safeguards, to secure district Data from unauthorized access, disclosure, alteration and use. The Consultant will use legally-required, industry standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing services pursuant to the Service Agreement. The Contractor will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Please describe where PII will be stored and the security protections taken to ensure PII will be protected and data security and privacy risks mitigated in a manner that does not compromise the security of the data: (a) Storage of Electronic Data (check all that apply): ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution

	☐ Other: (b) Storage of Non-Electronic Data: We do not anticipate storing non-electronic data (c)Personnel/Workforce Security Measures: 1) Background checks for personnel upon hire 2) Annual cybersecurity training 3) Annual ethics training (d) Account Management and Access Control: 1) Quarterly user access reviews 2) Endpoint detection and response solution 3) Annual penetration testing (e) Physical Security Measures: 1) Hosting centers are SOC 2 Type 2 audited 2) Data centers are designed to anticipate and tolerate failure while maintaining service levels. (f) Other Security Measures: 1) Date encrypted at rest and in transit 2) Email gateway to monitor for malicious content
Encryption	Data will be encrypted while in motion and at rest.

Riverside Insights
By: (Signature) Scott E. Olson
(Printed Name) Scott E. Olson
(Title) Manager of Proposal Services
Date: April 12, 2024

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Commack Union Free School District is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. The Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York State. The terms of the plan cannot conflict with any other terms of or Exhibits to the Data Privacy Agreement to which this Exhibit C is attached. **While this plan is not required to be posted to the District's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems. DO NOT LIMIT RESPONSES TO THE SPACES PROVIDED.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract	Contractor manages data, personnel, devices, systems, and facilities consistent with organizational objectives and the organization's risk strategy.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Riverside has a unified endpoint managemnet system to manage the security of devices. Controls on servers include encryption and regular backups
3	Specify how your officers, employees and Subcontractors who have access to PII pursuant to the Service Agreement will receive training on the federal and State laws that govern the confidentiality of PII.	Riverside provides cybersecurity training upon hire and annually theraefter. Employees also complete ethics training annually.
4	Outline the processes that ensure that your officers, employees and Subcontractors are bound by written agreement to the requirements of the Service Agreement, at a minimum.	Employees agree to obligations with respect to PII in their offer letters and the employee handbook, which is provided to employees upon hire and annually thereafter.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the District.	Riverside is committed to promptly notify relevant parties in the event of an incident. Such notice will include, to the extent known at the time, the type of data impacted, the individuals affected, and recommendations for precautions that should be taken.

6	Describe how data will be transitioned to the District when no longer needed by you to meet your contractual obligations, if applicable.	Access to data is available to the District at all times via the platform.
7	Describe your secure destruction practices and how certification will be provided to the District.	Upon the District's written request, Riverside will process the deletion request within 30 days of request and will provide confirmation of deletion.
8	Outline how your data security and privacy program/practices align with the District's applicable policies.	Riverside's security and privacy program is specifically designed to account for the requirements of New York Education Law 2-d and is in line with the District's Data Security and Privacy Policy.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	***YOU MAY USE TEMPLATE BELOW***

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Riverside leverages a unified endpoint management solution to manage assets in accordance with organizational objectives. The company also uses an endpoint management solution.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions	Riverside's various cybersecurity stakeholder groups, including IT, Legal, Product, and Digital, coordinate compliance and cybersecurity objectives to ensure they align with the organization's mission. This coordination involves the assignment of discreet roles and responsibilities.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Riverside develops, implements, and governs processes and documentation to facilitate an enterprise-wide privacy policy, which is reviewed and updated on an annual basis, as well as associated standards, controls, and procedures
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	As part of Riverside's data mapping process, the organization identifies areas of cybersecurity risk, which are then prioritized on a compliance road map. In addition, Riverside performs quarterly vulnerability scans of its applications and annual penetration testing.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Coordination between Legal/Compliance and business owners across the organization form the foundation of Riverside's risk management strategy, ensuring that broader cybersecurity program is aligned with business considerations and vice versa.

PROJECT (PR)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	Riverside has developed a plan for managing supply chain risks associated with the development, acquisition, maintenance and disposal of systems, system components and services. Specifically, responsible parties within the organization are required to conduct due diligence on suppliers before contracting with them and ensuring that any contract with a supplier addresses key risk areas.
	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	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.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Riverside personnel complete annual mandatory cybersecurity training that covers topics such as secure handling of PII/PHI, mitigating data breaches, and identifying attempts to secure unauthorized access to confidential information.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Data protection is an integral component of the organization's risk mitigation strategy. All customer data is encrypted in transit and at rest, and is hosted in secure data centers with industry-standard protections
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Information protection needs are technology-independent, required capabilities to counter threats to organizations through the compromise of information (e.g., loss of confidentiality, integrity or availability). Information protection needs are derived from the mission / business needs defined by the organization, the mission / business processes selected to meet the stated needs and the organizational risk management strategy.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Riverside requires asset custodians, in conjunction with data / process owners, to create, document, and implement maintenance procedures for technology assets.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Riverside's Tech Operations team manages the solutions that Riverside uses to ensure security and resilience of its systems. These solutions are provided by 3rd-party providers called Rapid7 and SentinelOne, and Riverside's data hosting providers also use their own security measures.
	Anomalies and Events (DE.AE):	

DETECT (DE)	Anomalous activity is detected and the potential impact of events is understood.	Riverside's endpoint protection solution, SentinelOne, provides threat hunting and neutralization capabilities.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Riverside deploys intrusion-detection and/or intrusion prevention technologies on critical systems.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	In order to gain the most complete situational awareness, Intrusion Detection / Prevention Systems (IDS/IPS) shall be deployed on critical systems, key network segments and network choke points. The organization employs automated tools to support real-time analysis of events. For critical systems, Riverside Insights cybersecurity personnel are responsible for correlating information and generating near real-time alerts from monitoring tools employed throughout the network to achieve organization-wide situational awareness.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Information system notifies organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events and takes organization-defined least-disruptive actions to terminate suspicious events.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	A cross-functional group, as well as relevant external stakeholders (e.g., insurers, outside counsel, third-party experts) would be involved in response activities in the event of a security incident.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Riverside is in the process of developing a breach notification testing protocol. This protocol will enable Riverside to run simulations of data security incidents and to make improvements based on the results of these tests.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Riverside's incident response procedure prevents expansion of an event, mitigates its effects, and promotes a prompt resolution of the incident
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Riverside incorporates lessons learned for contingency plans. Data/process owners and asset custodians are required to: (a) Perform a Root Cause Analysis following events that trigger usage of continuity plans; and (b) Incorporate lessons learned in updates to the continuity plans.
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Riverside relies on the incident detection and response tools of its hosting provider, AWS. These detection and response services are provided in connection with the data center hosting arrangements involving Riverside.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	As noted in the response to RS.IM, Riverside incorporates lessons learned in its contingency planning and general data privacy program.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Restoration activities would be coordinated with our third-party data center provider for our group platform, AWS. If notifications to customers is required, that would also be included in the restoration process.

Riverside Assessments, LLC dba Riverside Insights

Terms of Use

LAST UPDATED: December 19, 2023

Riverside Assessments, LLC dba Riverside Insights ("Riverside," "We," "Us," or "Our") provides content for Our assessments (collectively, the "Products") and related assessment management features via Our web-based platforms, including Riverside Elevate, Riverside Score, Riverside DataManager, the WJ IV Interpretation and Instructional Interventions Program (WIIIP), BDI-2 DataManager, and BDI-3 Mobile Data Solution (collectively, the "Platforms" and, together with the Products, the "Services").

These Terms of Use (the "Terms" or "Terms of Use") constitute a legal agreement concerning Riverside's Services and are between you, either as an individual or as an authorized representative on behalf of an organization, such as a school district, educational authority, university, clinic, hospital, or healthcare system ("You" or "Your"), and Riverside. Please note that different or additional terms may apply regarding your license of the Services if agreed to in writing between You and Riverside. If you are a user of the District version of easyCBM ("easyCBM"), please refer to the easyCBM Subscriber Agreement included in your easyCBM order form or presented to you at the time you completed your order for easyCBM ("Subscriber Agreement"). The Subscriber Agreement contains the terms and conditions applicable to your use of easyCBM.

PLEASE READ THESE TERMS OF USE CAREFULLY. BY ACCESSING, USING, OR DISPLAYING THE SERVICES, YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTAND, AND AGREE TO BE BOUND BY THESE TERMS OF USE AND TO THE COLLECTION AND USE OF YOUR INFORMATION AS SET FORTH IN RIVERSIDE'S ASSESSMENT PRIVACY POLICY (THE "PRIVACY POLICY"). DO NOT ACCESS, USE, OR DISPLAY THE SERVICES IF YOU DO NOT AGREE TO THESE TERMS AND THE PRIVACY POLICY.

1. Definitions

"**COPPA**" means the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6505, and the regulations promulgated thereunder, each as amended.

"DFARS" means the Department of Defense FAR Supplement, codified at 48 C.F.R. Parts 200-299.

"Effective Date" means the earlier of (i) the date You accept these Terms of Use (electronically or otherwise) or (ii) the date You first begin to use the Services.

"FAR" means the Federal Acquisition Regulation, codified at 48 C.F.R. Parts 1-52.

"FERPA" means the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and the regulations promulgated thereunder, each as amended.

"**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d *et seq.*, and the regulations promulgated thereunder, each as amended.

"**Term**" means the term during which these Terms of Use are in effect, which will begin on the Effective Date and continue for as long as You have access to the Services, subject to the termination and survival provisions of Section 11 (Term and Termination).

2. Access to Licensed Services

Subject to Your compliance with these Terms of Use and any accompanying user documentation, Riverside grants You a personal, limited, nontransferable, nonsublicensable, nonexclusive license to access and use the applicable Services during the Term. Riverside reserves the right, upon prior written notice to You, to discontinue versions of the Services. If a Service is discontinued, Riverside will notify you about whether a new version of such Service is available, and, if such version is available, You will be required to license the latest version of such Service in order to maintain access.

3. Access to the Platform

3.1 Required Computing Resources

Use of the Services requires, at a minimum, computing resources needed to access and browse the internet. Such computing resources may include, as specified in applicable user documentation: (i) a personal computer and/or mobile device; (ii) software, including browser software and operating system software; and (iii) other specified client-side computing resources (collectively, "Client-Side Computing Resources"). You are responsible for ensuring that You (a) have access to requisite Client-Side Computing Resources and (b) are sufficiently familiar with and trained regarding such Client-Side Computing Resources.

Riverside does not guarantee that the Services will operate with Your specific Client-Side Computing Resources. You are advised to carefully review each Service's posted minimum system requirements to ensure compatibility.

3.2 Enrollment Responsibilities

Depending on the specific Services You are using and your role with respect to such Services, You may need to select the users who will have access to the Services and prepare the necessary files to import or manually enroll such users employing features provided in the Services. For some Services, We may limit the number of users per subscription license.

3.3 Use of Passwords

Once enrolled, You will have the opportunity to create a password for Your assigned username ("Login Credentials"). All account users should have their own Login Credentials. Riverside will treat anyone who uses Your Login Credentials as You. Riverside will not be responsible for Your sharing or other misuse of Login Credentials, and Riverside will hold You responsible for the activities of a person using Your Login Credentials. You agree to maintain Your Login Credentials in confidence and to notify Riverside immediately if You know or suspect that someone is using Your Login Credentials in an inappropriate manner.

Riverside Insights

4. Riverside's Intellectual Property

Riverside's Services, including derived scaled scores based on the number of questions answered correctly for a given assessment ("Score Conversions"), reports of assessment results ("Reports"), and all related designs, layouts, appearances, and graphics therein, as well as the copyrights, trademarks, service marks, wordmarks, and logos contained within each of the foregoing, embody intellectual property rights owned by Riverside (or its licensors), including any rights under patent law, copyright law, trade secret law, and trademark law ("Riverside Intellectual Property"). All rights not expressly granted herein are reserved to Riverside or its licensors, as applicable.

5. Test Security; Use of Reports

Confidentiality is critical to the integrity, validity, and fairness of the testing process. Riverside restricts distribution of certain Products to qualified institutions and examiners. Under the *Standards for Educational and Psychological Testing* (2014) ("SEPT"), published by the American Educational Research Association, American Psychological Association, and National Council on Measurement in Education, educators and psychologists have a duty to protect the integrity of secured tests by maintaining the confidentiality of test questions and answers. Widespread dissemination of test protocols, which include substantial portions of the actual test items, would inevitably undermine this process. For this reason, Services are distributed only to recipients who agree to take appropriate steps to protect the confidentiality of the Services. Providing unauthorized third parties, including organizations or individuals providing test preparation or tutoring services, access to these Services; notetaking by non-professionals during test administrations; and the audio or video recording of test administrations would compromise test security and violate these Terms of Use. Such actions may result in the termination of Your rights to access and use the Services, as determined in Riverside's sole discretion.

You must use the Services in accordance with these Terms of Use and applicable federal, state, and local laws and regulations. You understand and agree that the Services are meant to be used as tools to support Your assessment process and are not intended or designed to replace Your professional judgment. You assume all responsibility for the use or misuse of the Services. You must use the Services in accordance with Riverside's Test Disclosure Policy and the SEPT (collectively, the "Policies and Standards").

6. Grant of Rights in Submitted Data and Feedback; Storage

By providing information to Riverside directly through Your use of the Services, including information about students/examinees and account usage data ("Submitted Data"), You grant Riverside a royalty-free, nonexclusive, transferrable, sublicensable, worldwide license to use the Submitted Data for all purposes contemplated under these Terms of Use as well as any user documentation. You acknowledge and agree that Riverside may use or disclose Submitted Data to provide maintenance and support for the Services and for communications relevant to your use of the Services, such as product updates, planned outages, maintaining sufficient licenses, and renewals. Riverside does not claim ownership in Submitted Data and retains only those rights in Submitted Data reasonably necessary or otherwise required to provide the Services and as otherwise contemplated under these Terms of Use and any user documentation. Submitted Data

that Riverside receives from You is subject to Section 14 (Riverside's Use of Submitted Data and Feedback; De-Identified Information) regarding use of de-identified data and the Privacy Policy.

In addition to the license You grant Us with respect to the Submitted Data, You grant Riverside a nonexclusive, worldwide, perpetual, royalty-free, irrevocable right to use, disclose, reproduce, modify, license, transfer, and otherwise distribute any comments, ideas, and suggestions for improvements or developments related to or associated with the Services that You provide ("Feedback") in any manner without compensation to You. Please do not submit Feedback if You do not wish to grant Us the rights set forth in this Section.

By providing Submitted Data and/or Feedback, You represent and warrant that You own such Submitted Data and/or Feedback (including intellectual property rights therein), or that You have obtained sufficient authority and right to the Submitted Data and/or Feedback in order to grant the rights to Riverside contemplated under these Terms of Use and any user documentation.

YOU ARE ADVISED TO EXPORT AND SAFEGUARD SUBMITTED DATA AND BACK UP IMPORTANT INFORMATION FREQUENTLY. If You choose to provide Submitted Data to Riverside via the Services, Riverside will periodically back up the Submitted Data and will take reasonable steps to securely store said backups. Notwithstanding anything to the contrary, You hereby release Riverside from any claim or liability relating to any failure in Riverside's database system and backup practices.

After expiration of the Term, Riverside will return or delete Submitted Data, in whole or in part, promptly after receiving written request and instruction from You or Your authorized designee, unless retention is necessary in Riverside's determination to provide other services to You; fulfill any other obligation it may owe You; or comply with applicable laws, regulations, court orders, or other legal processes. Riverside will retain all data that is not returned or deleted pursuant to the foregoing process in accordance with its standard records retention policy.

Notwithstanding anything in this Section, Riverside may retain Submitted Data in accordance with its backup or other disaster recovery policies and procedures. You acknowledge and agreed that backed-up data cannot be recovered following deletion. You unconditionally release, waive, and discharge any right or entitlement, whether by contract, under operation of law, or otherwise, to bring any cause of action or claim against Riverside now or in the future in connection with any data deletion request You make. You assume any and all risk of loss, liability, damage, expenses, or costs that may occur as a result of Your data deletion request.

7. Platform Availability and Errors

Riverside will use commercially reasonable efforts to make the Services available to You without significant interruption. At times the Services may be unavailable due to technical errors or for maintenance and support activities. We do not represent, warrant, or guarantee that the Services will always be available or are completely free of human or technological errors.

If a Service experiences a significant interruption that is not due to scheduled downtime, Riverside will use timely and commercially reasonable efforts to restore required functionality (the

"Availability Commitment"). The Availability Commitment does not apply to downtime: (i) due to emergencies; (ii) that Riverside otherwise schedules, for example, to install software updates and patches; (iii) due to Your violation of these Terms; or (iv) due to Your failure to update or upgrade your Services or the equipment you use to access the Services when suggested by Riverside.

The Services may contain typographical mistakes, inaccuracies, or omissions, and some information may not be complete or current. We expressly reserve the right to correct any errors, inaccuracies, or omissions and to change or update information at any time without prior notice. We do not make any representation or warranty concerning errors, omissions, delays, or defects in the Services or any information supplied to You via the Services, or that files available through the Services are free of viruses, worms, Trojan horses, or other code that include or manifest contaminating or destructive characteristics.

You may contact Riverside's technical support team with questions about the Services at the hours listed on our Support Page. In addition to taking reasonable steps to respond to reproducible errors or bugs in the Services commensurate with the severity of the error or bug, technical support may also provide You with information regarding Service availability.

8. Use Restrictions

You agree not to copy, duplicate, publish, distribute, display, modify, create derivative works of, or alter physical or electronic characteristics of the Services. You agree not to dismantle or reverse engineer or clone any part of the Services. You will not grant sublicenses to, assign, transfer, sell, or rent the Services or any sublicenses thereto without Riverside's prior written consent.

Because the Services, including Score Conversions and Reports, are Riverside Intellectual Property and are considered confidential information of Riverside, the Services will not be disclosed by You in response to requests made by third parties unless otherwise required pursuant to applicable law or valid court order, and then only after prior notice is provided to Riverside as well as an opportunity to prevent such disclosure. You agree that You will not otherwise, directly or indirectly, disclose any confidential information of Riverside without Riverside's prior written consent.

Subject to the restrictions in Section 5 (Test Security; Use of Assessment Score Reports), You may print, copy, display, and otherwise distribute Reports, but not any other parts of the Services, provided that such actions comply with Your obligations under the Policies and Standards and are otherwise in compliance with all applicable laws, regulations, and professional standards and obligations. You represent and warrant that You have obtained the necessary permissions from parents/guardians, students/examinees, and other applicable third parties relating to Your use of the Reports. You hereby release Riverside from any claim or liability relating to Your use of the Reports.

Notwithstanding anything to the contrary, You will not under any circumstance import any external content into any Reports or copy, display, or reproduce any test question from the Services without Riverside's prior written consent.

Riverside Insights

Your use of the Services to generate Reports is based on quantities of student administrations (record forms, answer documents, other consumable test or response booklets, digital administrations, or digital licenses) that You license from Riverside. You are only entitled to assess one student/examinee per record form, answer document, other consumable test or response booklet, digital administration, or digital license; however, multiple different Reports may be generated from a single test administration.

You agree that when using the Services, You will not: (i) introduce into the Services any virus, rogue program, time bomb, drop dead device, ransomware, back door, Trojan horse, worm, or other malicious or destructive code, software routines, denial of service attack, or equipment components designed to permit unauthorized access to the Services; (ii) otherwise harm other users, Riverside Intellectual Property, or any third parties; or (iii) authorize any third parties to perform any of the foregoing actions.

You will not use the Services to commit fraud or conduct other unlawful activities. You will not access or attempt to access any other person's account, personal information, or content without having the requisite permission or authority.

You will not use any bot, spider, or other automatic or manual device or process for the purpose of harvesting or compiling information about the Services or any users thereof for any reason.

You will not decrypt, transfer, frame, display, or translate (except translations for limited personal use authorized in writing by Riverside) any part of the Services.

You will not connect to or access any Riverside computer system or network without authorization.

You will not use the information in the Services to create or sell a similar product or service, or use the Services for the purpose of soliciting, selling, or offering services, merchandise, or products.

9. Third Party Websites

The Services may integrate with or provide links to other content, including websites or open education resources, on the Internet that We do not control. This content may provide opinions, recommendations, or other information from various individuals, organizations, or companies. We are not responsible for the nature, quality, or accuracy of such content. Inclusion of any linked content in the Services does not imply or express an approval or endorsement thereof by Us or of any of the opinions, treatments, information, products, or services provided in this content, even if We receive a referral fee in connection with Your use of such third-party content.

10. Limited Warranty

Riverside warrants that the Services will not infringe any valid United States copyrights existing at the time the Services are made available to You, provided that this warranty does not extend to any infringement arising out of: (i) the use of the Services in combination with systems, equipment, materials, content, or platforms not supplied by Riverside or any use of the Services

outside of the United States; (ii) Your use of the Services in violation of these Terms of Use the user documentation provided by Riverside, or any other agreement between You and Riverside; (iii) Your modification of the Services; (iv) Your failure to install or implement a released upgrade to the Services that would have avoided the infringement; or (v) any Submitted Data or Feedback. If You promptly notify Riverside of any such infringement claim brought by a third party of which You have knowledge or notice, and accord Riverside the right, at its sole option and expense, to handle the defense of the infringement claim, Riverside will defend You against such infringement claim and pay any final judgment or settlement thereof. Notwithstanding the foregoing, Riverside will not indemnify for any infringement claim that arises out of the scenarios set forth in clauses (i)-(v) of this Section. If such an infringement claim arises, or if Riverside becomes aware of the possibility of such a claim, then Riverside may, at its sole discretion (a) acquire the right for You to continue to use the affected Services in accordance with these Terms, (b) furnish You with a non-infringing replacement as soon as commercially possible, or (c) terminate these Terms in whole or in part by refunding any pre-paid, unused fees You paid for use of the Services. The obligations set forth in this Section are Your exclusive remedy and Riverside's sole obligations with respect to any breach of this warranty.

EXCEPT AS OTHERWISE EXPRESSLY STATED IN THIS SECTION 10 (LIMITED WARRANTY), THE SERVICES ARE PROVIDED "AS IS." RIVERSIDE MAKES NO WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED BY LAW, COURSE OF DEALING, COURSE OF PERFORMANCE, USAGE OF TRADE, OR OTHERWISE, WITH RESPECT TO THE SERVICES, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, RIVERSIDE DOES NOT WARRANT OR MAKE ANY PROMISES REGARDING THE CORRECTNESS, COMPLETENESS, SECURITY, USEFULNESS, ACCURACY, AVAILABILITY, OR RELIABILITY OF (I) YOUR USE THE SERVICES OR (II) ANY ADVICE YOU GLEAN OR INFER FROM THE SERVICES, WHETHER PROVIDED BY US OR A THIRD PARTY. WE DO NOT WARRANT (X) THAT THE SERVICES WILL BE UNINTERRUPTED, ERROR-FREE, OR FREE OF HARMFUL CODE; (Y) THAT THE SERVICES WILL MEET YOUR REQUIREMENTS OR ACHIEVE ANY INTENDED RESULT; OR (Z) THAT ANY DEFECTS WITH RESPECT TO THE SERVICES WILL BE CORRECTED.

11. Term and Termination

These Terms of Use are effective during the Term, subject to the termination and survival provisions of this Section 11 (Term and Termination).

Either party will have the right to terminate these Terms of Use if the other party breaches any of its obligations thereunder and fails to cure the same within thirty (30) days after receipt of written notice of default, except that there will be no cure period for Your breach of Riverside's rights under Section 4 (Riverside's Intellectual Property); Section 5 (Test Security; Use of Assessment Score Reports), Section 6 (Grant of Rights in Submitted Data and Feedback; Storage), or Section 8 (Use Restrictions). Upon termination of these Terms of Use, any rights You have in the Services will terminate.

The provisions of Section 4 (Riverside's Intellectual Property), Section 5 (Test Security; Use of Assessment Score Reports), Section 6 (Grant of Rights in Submitted Data and Feedback; Storage), Section 8 (Use Restrictions), Section 10 (Limited Warranty), Section 12 (Indemnification), Section

13 (Limitation of Liability), Section 14 (Riverside's Use of Submitted Data and Feedback; De-Identified Information), and Section 19 (General) will survive any expiration or termination of these Terms of Use. Riverside reserves the right to terminate these Terms of Use for convenience by providing You with reasonable notice and thereafter allowing You a reasonable opportunity (not to exceed 30 days) to export a copy of Your Submitted Data.

If these Terms of Use are terminated for any reason, Riverside may make a reasonable effort to grant You access to the Services for not more than thirty (30) days for the sole purpose of exporting Submitted Data (the "Submitted Data Retrieval Period"). Upon conclusion of the Submitted Data Retrieval Period, Riverside may destroy copies of Submitted Data in its possession.

If these Terms of Use expire, retention of Submitted Data will be governed by Section 6 (Grant of Rights in Submitted Data and Feedback; Storage).

12. Indemnification

EXCEPT TO THE EXTENT PROHIBITED BY APPLICABLE LAW, YOU AGREE TO INDEMNIFY, DEFEND, AND HOLD RIVERSIDE HARMLESS AGAINST ALL CLAIMS, ACTIONS, LIABILITIES, LOSSES, DEMANDS, DAMAGES, DEFICIENCIES, JUDGEMENTS, SETTLEMENTS, INTEREST, AWARDS, PENALTIES, FINCES, COSTS, OR EXPENSES (INCLUDING REASONABLE ATTORNEYS' FEES AND EXPENSES) ARISING OUT OF OR IN CONNECTION WITH: (I) YOUR USE OF THE SERVICES COVERED BY THESE TERMS AND/OR (II) YOUR FAILURE TO COMPLY WITH THESE TERMS.

13. Limitation of Liability

RIVERSIDE'S TOTAL AGGREGATE LIABILITY FOR LOSSES OR DAMAGES RELATING TO THESE TERMS OF USE AND/OR THE SERVICES, OR YOUR USE OR INABILITY TO USE THE SERVICES, REGARDLESS OF THE FORM OF ACTION, WILL IN NO EVENT EXCEED THE GREATER OF: (A) ONE THOUSAND U.S. DOLLARS (USD $1,000.00) OR (B) THE FEES ACTUALLY PAID BY YOU TO RIVERSIDE IN THE 12 MONTHS PRECEDING THE EVENT GIVING RISE TO THE LIABILITY.

IN NO EVENT WILL RIVERSIDE BE LIABLE TO YOU OR ANY THIRD PARTY, EITHER IN CONTRACT, TORT, OR OTHERWISE, FOR ANY INDIRECT, SPECIAL, PUNITIVE, ENHANCED, EXEMPLARY, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF FUTURE REVENUE, INCOME OR PROFITS, LOSS OF DATA, OR DIMINUTION IN VALUE, ARISING OUT OF OR RELATING TO YOUR USE OF THE SERVICES OR IN CONNECTION WITH ANY BREACH OF THIS AGREEMENT, REGARDLESS OF (X) WHETHER SUCH DAMAGES WERE FORESEEABLE, (Y) WHETHER RIVERSIDE WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND (Z) THE LEGAL OR EQUITABLE THEORY (CONTRACT, TORT, OR OTHERWISE) UPON WHICH THE CLAIM IS BASED.

THE LIMITATIONS SPECIFIED IN THIS SECTION 13 WILL SURVIVE AND APPLY EVEN IF ANY LIMITED REMEDY SPECIFIED IN THESE TERMS OF USE IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

14. Riverside's Use of Submitted Data and Feedback; De-Identified Information

Riverside may, from time to time, anonymize Submitted Data so that it constitutes de-identified Information ("De-Identified Information"). Riverside will only use De-Identified Information in accordance with HIPAA and FERPA and for lawful purposes, including quality assurance, product research and development, publications relevant to our Services and industry, norm development and validation, and other activities to develop, evaluate, improve, and demonstrate the effectiveness of our educational and clinical Services. The De-Identified Information will not directly identify a person but may be linkable to a particular computer, device, operation system, platform, or software instance (via a unique device ID or otherwise) ("Usage Information"). You acknowledge and agree that Riverside will be free to use De-Identified Information, in compliance with HIPAA and FERPA requirements, for the purposes described in these Terms of Use.

15. Protection of Student Personal Information

Please see the Privacy Policy governing your license of our Services for information about (i) Our practices related to collection, use, and deletion of personal information, including how You can access, review, and update personal information, and (ii) the security measures We have in place designed to safeguard your information.

16. Applicability of HIPAA

If You are a "Covered Entity" as defined under HIPAA, You and Riverside agree that the Business Associate Addendum will govern HIPAA-related matters (click here to review the Business Associate Addendum). If You are not a Covered Entity, this Section does not apply.

17. Federal Government Terms and Conditions

If You are the United States Government or any agency, subdivision, or instrumentality thereof (the "U.S. Government"), the Services (including any related databases, documentation, technical data, and programmer's tools) delivered to the U.S. Government are "commercial computer software" or "commercial technical data" pursuant to the applicable FAR, DFARS, or other agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation of the Services are subject to these Terms of Use, pursuant to FAR 12.212 (Computer Software) and 12.211 (Technical Data), as applicable. If You are the U.S. Government and subject to the DFARS, then the Services (including any related databases, documentation, technical data, and programmer's tools) is provided subject to DFARS 252.227-7015 (Technical Data—Commercial Items) and DFARS 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation), as applicable. Should the Services be deemed to not constitute "commercial computer software" or "commercial technical data," then they will be given to the U.S. Government with "Limited Rights" or "Restricted Rights" (as defined under DFARS), as applicable. In all cases, these Terms of Use supersede any conflicting terms or conditions in any government order document; provided, any provisions contained herein contrary to applicable mandatory federal laws will be treated as provided in FAR 52.212-4(u).

18. Consent Regarding Students' Personal Information

Please note that FERPA requires parental/guardian consent before a service provider, such as Riverside, is given access to personal information contained in a student's/examinee's

educational records. Under FERPA, this parental/guardian consent requirement is met where the service provider acts as a type of "school official" by performing services for the school that would otherwise be performed by the school's own employees. Riverside fulfills FERPA requirements for qualifying as a school official by, among other steps, giving schools direct control with respect to the use and maintenance of the educational records at issue (including associated personal information) and refraining from re-disclosing or using this personal information except for purposes of providing the Services or as required by applicable laws, regulations, court orders, or other legal processes. Riverside will comply with access requests as required by FERPA.

19. General

THESE TERMS WILL BE GOVERNED BY AND INTERPRETED IN ACCORDANCE WITH THE LAWS OF THE STATE OF ILLINOIS, WITHOUT GIVING EFFECT TO ANY CHOICE OF LAW OR CONFLICT OF LAW PRINCIPLES OR RULES (WHETHER UNDER THE LAWS OF THE STATE OF ILLINOIS OR OF ANY OTHER JURISDICTION) TO THE EXTENT SUCH PRINCIPLES OR RULES WOULD REUQIRE OR PERMIT THE APPLICATION OF THE LAWS OF ANY JURISDICTION OTHER THAN THOSE OF THE STATE OF ILLINOIS. The foregoing choice of law notwithstanding, copyright, trademark, and patent claims are subject only to U.S. Federal law and U.S. Federal court interpretation thereof. You agree that any action at law or in equity arising out of or relating to these Terms of Use will be filed only in the state or federal courts located in the Northern District of Illinois, Eastern Division. These Terms will not be assignable by You, either in whole or in part. Riverside reserves the right to assign the rights and obligations under these Terms of Use for any reason and in Riverside's sole discretion. The Privacy Policy must be read in conjunction with these Terms of Use, and the provisions of the Privacy Policy are incorporated herein. These Terms of Use and the Privacy Policy constitute the entire agreement between You and Riverside concerning the Services, your use thereof, and any related activities, and supersede all discussions, proposals, bids, understandings, agreements, invitations, orders, and other communications, oral or written, on this subject. These Terms may not be waived, amended, or modified in any way without the prior written permission of Riverside. We may revise and update these Terms of Use from time to time and will post the revised terms of use to Our website and may also post links to them on Our Platforms. UNLESS OTHERWISE STATED IN THE AMENDED VERSION OF THESE TERMS OF USE, ANY CHANGES TO THESE TERMS OF USE WILL APPLY IMMEDIATELY UPON POSTING. We are not obligated to provide You with notice of any changes, and any changes to these Terms of Use will not apply retroactively to events that occurred prior to such changes. Your continued use of the Services will constitute Your agreement to any new provisions within the revised terms of use. You may print a copy of these Terms of Use and the Privacy Policy for Your records. If any one or more provisions of these Terms of Use are found to be illegal or unenforceable, the remaining provisions will be enforced to the maximum extent possible. To the extent any licensed order from You conflicts with or amends these Terms of Use in any way, these Terms of Use, as unmodified, will prevail. To the extent the Privacy Policy conflicts with or amends these Terms of Use in any way, the Privacy Policy will prevail.

Any license granted under these Terms of Use to You must be expressly provided herein, and there will be no licenses or rights implied hereunder, based on any course of conduct or other construction or interpretation thereof. All rights and licenses not expressly granted to You by Riverside are reserved.