

Richland County School District One
Data Confidentiality and Security Agreement for Service Providers

_____ (Provider”) hereby agrees to the terms of this Data Confidentiality and Security Agreement (“Security Agreement”) for the purpose of sharing confidential student and/or employee information between Richland County School District One (“RICHLAND ONE”) and Provider to protect personally identifiable information and other regulated data exchanged between them as required by applicable state and federal laws and regulations, such as, with regard to student data specifically, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g and its implementing regulations at 34 CFR part 99; the Protection of Pupil Rights Amendment (PPRA), 20 U.S.C. 1232h and its implementing regulations at 34 CFR part 98; and the Children’s Online Privacy Protection Act (COPPA), 15 U.S.C. 6501-6506; as well as RICHLAND ONE Board Policies and their accompanying regulations and procedures.

- 1. Purpose.** RICHLAND ONE is a local education agency that maintains confidential information of its employees and students, including student “educational records” as defined under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g, and its implementing regulations at 34 CFR part 99; RICHLAND ONE Board Policies; and other applicable law. Provider is requesting access to certain data maintained by RICHLAND ONE for the purpose of providing educational services and/or instructional technology products to RICHLAND ONE, as described herein. The purpose of this Security Agreement is to set forth the terms and conditions upon which Provider may be granted access to such data in order to ensure that the data is used and stored appropriately and in compliance with all applicable federal, state, and local laws, regulations, and policies.
- 2. Student or Employee Records and Information.** Provider acknowledges that any data shared and released to Provider by RICHLAND ONE (the “Shared Data”) is for the sole purpose of providing educational services to enhance, supplement, and improve instruction for students within RICHLAND ONE or providing employee related services as described in Attachment 1. The Shared Data is defined as any data or information shared with Provider pursuant to this Agreement, including but not limited to any de-identified data, aggregated data sets, personally identifiable information (PII) about students or employees, and other student or employee information, including, but not limited to, first and last name, birthdate, home address, telephone number, email address, student discipline records, grades, test results, student generated content (to include but not limited to essays, research projects, creative writing, art, music, and other information to which a student may claim ownership); student special education data, evaluations, criminal records, medical records, health records, social security numbers, text messages, documents, other identifiers, search activity, images, audio or video recordings, student parents’ names, or any other information or identification number that would provide information about a specific student or employee including metadata and user content. Shared Data that pertains to students includes “Personally Identifiable Information (PII),” as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law and shall constitute Education Records for the purposes of this Security Agreement, and for the purposes of federal, state, and local laws and regulations. Shared Data will be used by Provider for the sole purpose of providing the services described in **Attachment A**, and for improving services

under this Agreement. The parties agree that the Shared Data and all rights to the Shared Data, including all intellectual property rights, shall remain the exclusive property of RICHLAND ONE, and that Provider has a limited, nonexclusive, license solely for the purpose of performing its obligations as outlined in this Agreement.

- 3. Compliance with Applicable Laws, Policies, and Procedures.** To become or remain a recipient of the Shared Data, Provider agrees to comply with the provisions of FERPA, PPRA, COPPA, and all other applicable laws and regulations in all respects related to student records. For purposes of this Security Agreement, FERPA includes 20 U.S.C. 1232g, Chapter 99 of Title 34 of the Code of Federal Regulations, and any Richland County School District One policies and procedures implementing these federal laws. PPRA includes 20 U.S.C. 1232h, Chapter 98 of Title 34 of the Code of Federal Regulations, and any state law and Richland County School District One policies implementing these federal laws. COPPA includes 5 U.S.C. 6501-6505, Chapter 312 of Title 16 of the Code of Federal Regulations, and any state law, regulation and/or Richland County School District One policies implementing these federal laws. Nothing in this Security Agreement may be construed to allow Provider to maintain, use, or disclose any Shared Data in a manner inconsistent with any applicable law, regulation, or policy.
- 4. Authorized Use of Shared Data.** All services provided by Provider shall at all times be limited to institutional functions of RICHLAND ONE that could otherwise be provided by a school official and which RICHLAND ONE is “outsourcing” to Provider pursuant to 34 CFR 99.31(a)(1)(B). Provider agrees to use the Shared Data for no other purpose other than those identified in Paragraph 2 of this Agreement. Provider understands that the Security Agreement does not convey ownership of Shared Data to Provider. All Shared Data transmitted to the Entity pursuant to the Service Agreement is and will continue to be the property of RICHLAND ONE. The disclosure of Shared Data to Provider is not an assignment of ownership of the Shared Data to the Entity. Provider specifically acknowledges that Provider’s marketing activities are not an authorized use of the Shared Data.
- 5. Procedures for the Maintenance and Security of Shared Data.** While in the possession, custody, or control of Provider, all Shared Data shall be stored in a secure environment with access limited to the least number of staff needed to complete the work requested by RICHLAND ONE. Provider shall develop, implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the confidentiality, integrity, and availability of all electronically maintained or transmitted data received from, or on behalf of, RICHLAND ONE. Such measures shall include processes for transmission and storage of such data.

 - a. Provider agrees that it will protect the Shared Data against loss, destruction, and unauthorized uses or disclosures according to industry best practices and no less rigorously than it protects its own confidential information. Specifically, Provider agrees that all student records and PII obtained in the course of providing services to RICHLAND ONE shall be subject to the confidentiality and disclosure provisions of applicable federal and state statutes and regulations, and Richland County School District One policies, including but not limited to the laws and policies described in

Paragraph 3 of this Security Agreement.

- b. For the purposes of ensuring Provider 's compliance with this Security Agreement and all applicable state and federal laws, Provider shall designate one or more individuals as the primary data custodian(s) of the data that RICHLAND ONE shares with Provider and shall notify RICHLAND ONE of the name(s) and title(s) of such individual(s) prior to any data being shared. RICHLAND ONE will release all data and information for this project to the named primary data custodian(s). The primary data custodian(s) shall ensure that the project shall be conducted in a manner that does not permit personal identification of RICHLAND ONE students or employees by anyone other than representatives of Provider who need such information for the purposes described in Paragraphs 1 and 2 of this Security Agreement. The primary data custodian(s) shall also be responsible for maintaining a log of all Shared Data received pursuant to this Security Agreement and confirming in the log the timely destruction or return of the Shared Data in accordance with this Security Agreement and any applicable state or federal law.
- c. Provider shall use industry best practices to protect RICHLAND ONE data from unauthorized physical and electronic access no less rigorously than it protects its own confidential information. All RICHLAND ONE data shall be kept in a secure location preventing access by unauthorized individuals. Provider shall not forward to any person or entity other than RICHLAND ONE any employee or student record or PII, including, but not limited to, the employee or student's identity, without the advance written consent of RICHLAND ONE. Provider agrees to handle any and all Shared Data using appropriate access control and security, including password-protection and encryption in transport and electronic storage, and periodic auditing of data at rest. Data subject to FERPA shall not be emailed in plain text or used for marketing campaigns. Provider will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.
- d. Provider will maintain an access log delineating the date, time, and identity of any person or entity given access to any Shared Data who is not in the direct employ of Provider. No such access shall be granted except in strict compliance with the terms and conditions of this Agreement and applicable law.
- e. Subject to applicable law and upon receipt of a request from RICHLAND ONE, Provider must return and/or destroy all Shared Data received from RICHLAND ONE in Provider's possession or control and remove all Shared Data from Provider's systems, including, but not limited to servers, workstations, storage media, and backup media unless otherwise specifically agreed. Provider shall not retain copies of any Shared Data received from RICHLAND ONE. Provider shall ensure that they will dispose of any and all Shared Data in its possession or control received from RICHLAND ONE in manner that maintains the confidentiality of the contents of such records (e.g., shredding paper records, erasing and reformatting hard drives, erasing and/or physically destroying any portable electronic devices). The primary data custodian(s) must confirm the removal/destruction of all Shared Data in Provider's

possession or control in accordance with this Security Agreement and any applicable state and federal law.

6. Prohibition on Unauthorized Use or Disclosure of Shared Data.

- a. Provider agrees to hold all Shared Data in strict confidence. Provider shall not use or disclose such data received from or on behalf of RICHLAND ONE except as authorized in writing by RICHLAND ONE or as required by law. Provider agrees not to disclose any data obtained from RICHLAND ONE in a manner that could identify any individual student or employee to any other entity, attempt to infer or deduce the identity of any individual student or employee based on data provided by RICHLAND ONE, or claim to have identified or deduced the identity of any student based on data provided by RICHLAND ONE.
- b. Data containing personally identifiable information about RICHLAND ONE students or staff may not be stored on any server or other device outside the physical and political borders of the United States. Such data may not be subject to access, confiscation or use outside the laws of the United States. Such data must be stored and maintained physically where only the laws of the United States may be applied to access, use or confiscation or seizure. Such data may not be controlled by a company or individual that is not subject to the laws of the United States. Upon request, RICHLAND ONE shall be provided a list of locations where Provider stores Shared Data
- c. Provider is prohibited from mining Shared Data for any purposes other than those agreed to in advance in writing by RICHLAND ONE. Data mining or scanning of user content for the purpose of advertising and/or marketing to students or their parents is strictly prohibited.
- d. In no event will Provider use any of the Shared Data for its own commercial marketing, advertising or solicitation purposes, or for the commercial marketing, advertising or solicitation purposes of any third-party. Provider will not use any Shared Data to advertise, market or solicit to RICHLAND ONE students or their parents. Section 30-2-50 of the Code of Laws of the State of South Carolina provides that no person or private entity shall knowingly obtain or use any personal information obtained from a public body for any commercial solicitation directed to a person in this state. RICHLAND ONE, as a public entity, gives notice to Provider, as a potential recipient of records from RICHLAND ONE, that obtaining or using these public records for commercial solicitation is prohibited.
- e. Immediately upon discovery of any suspected or actual data security breach involving the unauthorized release to or acquisition by a third party of Shared Data potentially affecting or compromising the security or confidentiality of Shared Data or resulting in a violation of any term of this Agreement, Provider shall take all commercially reasonable efforts to limit and mitigate such data security breach to the extent possible. Provider further agrees to notify District of the breach in the most expedient time

possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notice to RICHLAND ONE shall include the following information:

- i. The date(s) or date ranges of the breach;
- ii. a general description of the manner of the breach
- iii. the type of information that was or believed to have been subject to the breach
- iv. Who made the unauthorized use or received the unauthorized disclosure,
- v. What Provider has done or shall do to mitigate the effects of the unauthorized use or disclosure, including information related to the involvement of law enforcement, if any; and
- vi. What corrective action Provider has taken or shall take to prevent future similar unauthorized use or disclosure.

Provider shall also provide such other information related to the unauthorized use or disclosure that may be reasonably requested by RICHLAND ONE. RICHLAND ONE also may require that Provider provide a written notice of the breach or disclosure, as well as a description of the corrective actions taken, to any RICHLAND ONE student, parent, or employee directly impacted by the breach or disclosure as well as any applicable state or federal entity to which reporting is required. Any such notice shall be subject to review and prior approval by RICHLAND ONE.

- f. Provider may use de-identified, aggregated Shared Data for product development and research purposes only as specifically authorized and consented to in advance in writing by RICHLAND ONE. Any such de-identified data will have all direct and indirect personal identifiers removed, including, but not limited to, name, ID numbers, date of birth, demographic information, location information, and school ID. Provider agrees not to attempt to re-identify any de-identified data and not to transfer de-identified data to any other party without RICHLAND ONE express written consent.
- g. Provider will not release any research or publications pertaining to RICHLAND ONE's data without RICHLAND ONE's advance written consent.

7. Employees, Contractors, and Agents. Provider may share any of the Shared Data with any of its subcontractors only with the advance written permission of RICHLAND ONE. Any such request from Provider shall be in writing and shall identify the person(s) or entities to whom disclosures will be made and the purposes of the disclosures. Should RICHLAND ONE, in its sole discretion, approve any such request, Provider shall ensure that each approved subcontractor is contractually bound to adhere to all of the terms of this Security Agreement with respect to its possession and use of any Shared Data and is aware of its obligations under applicable law with regard to the possession, use and re-disclosure of any PII. Any such agreement between Provider and its subcontractor(s) shall be subject to review and approval by RICHLAND ONE before any Shared Data is disclosed to the subcontractor(s). Nothing in this paragraph shall relieve Provider of any its obligations under this Agreement, including its responsibilities to ensure the security of any Shared Data provided by RICHLAND ONE pursuant to this Agreement.

8. Monitoring and Auditing. Any Shared Data held by Provider will be made available to RICHLAND ONE for review and inspection upon request of RICHLAND ONE. Provider shall cooperate with RICHLAND ONE or with any other person or agency as directed by RICHLAND ONE, in monitoring, auditing, or investigating activities related to Provider's use and safeguarding of the Shared Data, including but not limited to allowing inspection of the data logs described in Paragraph 5.b and 5.d of this Agreement. RICHLAND ONE and its auditors will maintain the confidentiality of any trade secrets of Provider that may be accessed during an audit conducted under this Security Agreement.

9. Term; Post-Termination. This Security Agreement takes effect upon the date of full execution and continues in full force and effect for so long as Provider and its subcontractor(s) if any, has possession, custody, or control of any of the Shared Data. Upon the termination of the subscription to the instructional system provided by Provider and/or any other contract, purchase order, agreement or terms of service between RICHLAND ONE and Provider, all Shared Data shall, at RICHLAND ONE's sole option, be destroyed or returned to RICHLAND ONE. No other entity, including any subcontractors of Provider, shall be authorized to continue possessing or using any Shared Data. Any Shared Data remaining on any computers, servers, or other technological devices of Provider or its employees, agents, or subcontractors, shall be permanently deleted.

10. Breach and Default; Indemnification; Remedies.

- a. In the event of a material data or security breach, or, if RICHLAND ONE determines, in its sole discretion, that student information has been mishandled or disclosed in a manner inconsistent with this Security Agreement, RICHLAND ONE may immediately cancel any and all agreements with Provider and demand the immediate return or destruction of any and all of the Shared Data.
- b. Provider shall fully indemnify and hold harmless the Richland County School District One and its past, current and future members, agents, employees and Board of Trustees, from and against all claims, actions, demands, costs, damages, losses, and/or expenses of any kind whatsoever proximately resulting from any material data breach of this Security Agreement or any unauthorized use or disclosure of the Shared Data by Provider or its subcontractor(s). This section shall survive the expiration or earlier termination of this Security Agreement.
- c. Nothing in this Agreement shall restrict RICHLAND ONE from seeking any other rights or remedies to which it may be entitled at law or equity.

11. No Right or Entitlement to Shared Data. This Security Agreement sets out the terms and conditions, under which RICHLAND ONE may, in its sole discretion, provide Shared Data to Provider. Nothing in this Security Agreement creates any right, title, or interest in Provider to receive any such information.

12. Miscellaneous.

- a. Governing Law. This Security Agreement and the rights and obligations of the parties hereto shall be governed by and construed and enforced in accordance with the laws of the State of South Carolina.
- b. No Third Party Beneficiaries. Nothing in this Security Agreement shall confer upon any person other than the parties any rights, remedies, obligations, or liabilities whatsoever.
- c. Counterparts. This Security Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.
- d. Headings. The headings and other captions in this Security Agreement are for convenience and reference only and shall not be used in interpreting, construing or enforcing any of the provisions of this Security Agreement.
- e. Assignment of Rights. Neither this Security Agreement, nor any rights, duties, nor obligations described herein shall be assigned by Provider without the prior express written consent of RICHLAND ONE.
- f. Entire Agreement; Amendment. This Agreement contains the entire agreement between the parties and supersedes any previous agreements and proposals, oral or written, related to the subject matter hereof. Any modification or amendments to this Agreement shall be effective only if made in writing and signed by both parties.
- g. Conflicts. In the event of any conflict between this Security Agreement and any existing or future contract, purchase order, agreement or terms of service between RICHLAND ONE and Provider, the terms and conditions of this Security Agreement shall control.
- h. Severability. If for any reason a court of competent jurisdiction finds any provision or portion of this Agreement to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remainder of this Agreement will continue in full force and effect.
- i. Waiver. The failure or delay of any party to enforce any of the provisions of this Agreement will not be construed to be a waiver of the right of such party thereafter to enforce such provisions.

IN WITNESS THEREOF, the parties to this Agreement have set their hands and seals on the dates indicated below.

**Richland County School District
One**

PROVIDER

Authorized Signature

Authorized Signature

Date

Date