Version 2
Revised: Nov 15, 2023

North Carolina Department of
PUBLIC INSTRUCTION

Data Confidentiality and Security Agreement for Online Service Providers and Public School Units

(Student Data)

________________________________(“Provider”) hereby agrees to the terms of this Data Confidentiality

and Security Agreement (“Security Agreement”) for the purpose of sharing confidential student information

between The Charlotte-Mecklenburg Board of Education (“Public School Unit” or “PSU” as defined by N.C. Gen. Stat. 115C-5(7a)) and Provider in a manner consistent with any applicable laws and policies, including, but not limited to, 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; the Children’s Online Privacy Protection Act (COPPA), 15 U.S.C. 6501-6506 and its implementing regulations at 16 CFR part 312; N.C. Gen. Stat. §§ 115C-401.1, 115C-401.2, and 115C-402. The Provider also agrees to abide by any local policies set forth by the Public School Unit.

1. **Purpose**. The North Carolina Department of Public Instruction is charged with maintaining statewide student data systems and protecting student data under North Carolina General Statute 115C, Article 29 Provider is requesting access to certain student data maintained by NCDPI and Public School Unit for services rendered by the Provider. The purpose of this Security Agreement is to set forth the terms and conditions upon which Provider may be granted access to such student data in order to ensure that the student data is used and stored appropriately and in compliance with all applicable federal, state, and local laws, regulations, and policies. The Provider shall receive fields and data described in Attachment A.

2. **Student Records and Information.** Provider acknowledges that any data shared and released to Provider by the Public School Unit (the “Shared Data”) is for the purpose of providing the goods and services purchased by the PSU. 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, and other student information, including, but not limited to, student data, metadata, and user content. The Shared Data will be used by Provider for the purpose of populating student data into systems subscribed to by the Public School Unit . The parties agree that the Shared Data and all rights to the Shared Data shall remain the exclusive property of NCDPI and the Public School Unit, and that Provider has a limited, nonexclusive, license solely for the purpose of performing its obligations under agreements with the PSU.

3. **Compliance with Applicable Laws, Policies, and Procedures**. To become or remain a recipient of the Shared Data, Provider agrees to comply with all applicable laws and regulations in all respects. 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 North Carolina State Board of Education policies, local Public School Unit Board of Education 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, State Board of Education or Public School Unit 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 and PSU Board of Education policies implementing these federal laws. Nothing in this Security Agreement may be construed to allow the 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 functions of the Public School Unit that could otherwise be provided by a school official and which the Public School Unit 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. The Security Agreement does not convey ownership of Shared Data to Provider.

5. **Procedures for the Maintenance and Security of Shared Data**. While in the possession, custody, or control of the Provider, or any authorized subcontractor, all Shared Data shall be stored in a secure environment, within the continental United States, with access limited to the least number of staff needed to complete the work requested by the PSU. The 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 the PSU. Such measures shall include processes for the transmission and storage of such data.

    a. Provider agrees that it will protect the Shared Data against loss, unauthorized destruction, erasure and unauthorized uses or disclosures. Specifically, Provider agrees that all Shared Data received or accessed in the course of providing services to the PSU shall be subject to the confidentiality and disclosure provisions of the NC Public Records Act and other applicable federal and state statutes and regulations, and PSU 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 the PSU shares with Provider and shall notify the PSU of the name(s) and title(s) of such individual(s) prior to any disclosure of any Shared Data to such persons, and in the event of any changes to the named individuals. The PSU will release all Shared Data 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 PSU students 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 ensuring the timely destruction or return of the Shared Data as required by this Security Agreement.

    c. Provider shall protect Shared Data from unauthorized physical and electronic access. All Shared Data shall be kept in a secure location, within the continental United States, preventing unauthorized access. Provider shall not forward to any person or entity other than the contracted PSU any student record or PII, including, but not limited to, the student's identity, without the advance written consent of the PSU.

d. 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 such Data at rest. Data subject to FERPA shall not be emailed in plain text or used for marketing campaigns.

e. Provider will maintain an access log delineating the date, time, and identity of any person or entity given access to any Shared Data student records 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.

6. **Required Documentation**

a. Provider agrees to provide the PSU with a completed self-assessment using an approved self-assessment toolkit prior to the execution of the contract. **The list of approved self-assessment toolkits are listed at:** https://www.dpi.nc.gov/about-dpi/technology-services/third-party-data-integration.

b. Provider agrees to provide the PSU, at the execution of the contract and annually thereafter, a third-party conducted assessment reports. The list of approved third-party conducted assessments are listed **at:** https://www.dpi.nc.gov/about-dpi/technology-services/third-party-data-integration.

7. **Additional Security Measures and Documentation.** Provider agrees to adhere to the guidelines set forth in the North Carolina Information Security Manual, located at https://it.nc.gov/documents/statewide-information-security-manual. The PSU, at their sole discretion, may request additional documentation including:

a. A credentialed vulnerability scan of the environment with all medium and above vulnerabilities remediated in accordance with state security requirements. This scan must be current within the last 30 days. Provider agrees to provide this information to PSU, at the execution of the contract and annually thereafter, as requested by the PSU.

b. A third-party conducted penetration test, dated within the last 12 months, with all medium and above findings remediated in accordance with state security requirements. Provider agrees to provide the PSU, at the execution of the contract and annually thereafter, as requested by the PSU.

c. The provider shall securely share any documentation provided with the North Carolina Department of Public Instruction for evaluation and review at the request of the Department of Public Instruction.

8. **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 the contracted PSU except as authorized in writing by the contracted PSU or as required by law. Provider agrees not to disclose any data obtained from the contracted PSU in a manner that could identify any individual student to any other entity, attempt to infer or deduce the identity of any individual student based on data provided by the PSU, or claim to have identified or deduced the identity of any student based on data provided by the PSU.

b. Provider agrees and specifically warrants that it, its officers, directors, principals and employees, and any subcontractors, shall hold all information received during performance of this Contract in the strictest confidence and shall not disclose the same to any third party without the express written approval of the State.

c. Provider is prohibited from mining Shared Data for any purposes other than those agreed to in writing by DPI and the Public School Unit. Data mining or scanning of user content for the purpose of advertising and/or marketing to students or their parents is strictly prohibited by NCGS § 115C-401.2.

d. In no event will Provider use any of the Shared Data for its own commercial marketing or advertising purposes, or for the commercial marketing or advertising purposes of any third party. Provider also agrees to not market additional or add-on services to parents or students within the Public School Unit, without the express written consent of the PSU.

e. In the event of any unauthorized use or disclosure of Shared Data, Provider shall report the incident to the PSU no more than one (1) business day after Provider learns of such use or disclosure and shall cooperate with any investigations conducted by Law Enforcement, the PSU, the North Carolina Department of Public Instruction, the North Carolina Department of Information Technology, and any affiliated parties. As used herein, incident includes a Cybersecurity Incident or Significant Cybersecurity Incident as defined in NC General Statute 143B-1320. Unauthorized disclosure shall include, but is not limited to, technical breaches, misconfigurations, invalid permissions, and any other access which results in a user of the system or public receiving access to data they would not otherwise be entitled to.

f. Provider shall provide a report within two (2) business days upon PSU request of the current state of the incident. Provider will also provide an incident postmortem report within two (2) business days of incident resolution. Such report shall identify:

i. The nature of the unauthorized use or disclosure,

ii. The Shared Data used or disclosed,

iii. Who made the unauthorized use or received the unauthorized disclosure,

iv. What Provider has done or shall do to mitigate the effects of the unauthorized use or disclosure, and

v. What corrective action Provider has taken or shall take to prevent future similar unauthorized use or disclosure.

g. Provider shall also provide such other information related to the unauthorized use or disclosure that may be reasonably requested by NCDPI and the PSU within no more than one (1) business day of the request. NCDPI and/or the PSU may also require that Provider provide a written notice of the breach or disclosure, as well as a description of the corrective actions taken, to any student, parent, or employee directly impacted by the breach or disclosure. Any such notice shall be subject to review and approval by NCDPI and the PSU.

h. Provider will not release any research or publications pertaining to the Public School Unit's data without the PSU's advance written consent

i. NCDPI acknowledges that Provider may consider certain information reported pursuant to e and f above as confidential and not subject to disclosure under the NC Public Records Act. Provider may mark such information as exempt from disclosure upon consultation with Provider's legal counsel, however such determination shall not preclude delivery of the information to NCDPI.

9. Employees, Contractors, and Agents. Provider may share any of the Shared Data with any of its subcontractors only with the advance written permission of the Public School Unit. Any such request from Provider shall be in writing and shall identify the person(s) or entit(ies) to whom disclosures will be made and the purposes of the disclosures. Should the PSU, in their 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 the Public School Unit before any Shared Data is disclosed to the subcontractor(s). Nothing in this paragraph shall relieve the Provider of its obligations under this Agreement, including its responsibilities to ensure the security of any Shared Data provided by the PSU pursuant to this Agreement.

10. Monitoring and Auditing. Any Shared Data held by Provider will be made available to PSU for review and inspection upon request of the PSU. Provider shall cooperate with the PSU or the or with any other person or agency as directed by the PSU, 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. The Public School Unit will maintain the confidentiality of any trade secrets of Provider that may be accessed during an audit conducted under this Security Agreement. The PSU reserves the right to terminate this Security Agreement at any time if the Provider does not comply with the terms and conditions set forth herein.

11. Term; Post-Termination. This Security Agreement takes effect upon the date of full execution and continues in full force and effect while Provider has possession, custody, or control of any of the Shared Data. Within 90 days of the expiration of the Subscription, Purchase Order, or Terms between the PSU and the Provider - or upon notice of termination of this agreement - the Provider shall assist the PSU, upon written request, in extracting and/or transitioning all Data collected by the Provider in the format determined by the PSU. The Transition Period may be modified in writing by the parties in a contract amendment. Upon termination and after providing the Data to the PSU, the Provider shall permanently destroy or render inaccessible any Shared Data and provide the state notice in writing. All plugins and data sharing of PSU data to the Provider will terminate immediately. No other entity, including any subcontractors of Provider, shall be authorized to continue possessing or using any Shared Data. Any data remaining on any computers, servers, or other technological devices of Provider or its employees, agents, or subcontractors, shall be permanently deleted. Provider shall complete such destruction as promptly as possible, but not less than thirty (30) days after the effective date of the termination or expiration of this Agreement. Within such thirty (30) day period, Provider shall certify in writing to PSU that such destruction has been completed. This section shall survive the expiration or earlier termination of this Agreement.

12. Breach and Default; Indemnification; Remedies.

   a. In the event of a material data or security breach, or, if the PSU determines, in their sole discretion, that student information has been mishandled or disclosed in a manner inconsistent with this Security Agreement, the PSU may demand the immediate return or destruction of any and all of the Shared Data.

   b. Provider shall fully indemnify and hold harmless the State Board of Education, the Department of Public Instruction, and the District and its past, current and future members of Boards of Education, elected officials, agents, and employees 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).

c. Nothing in this Agreement shall restrict the PSU from seeking any other rights or remedies to which it may be entitled at law or equity.

13. No Right or Entitlement to Student Data. This Security Agreement sets out the terms and conditions, under which the PSU may, in their 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.

14. 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 North Carolina.

b. Relationship of Parties. The parties shall be independent contractors, and nothing herein shall be construed as creating a partnership or joint venture; nor shall any employee of either party be construed as employees, agents, or principals of any other party hereto.

c. 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.

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 the PSU.

f. Severability. If any provision of this Agreement shall be declared invalid or unenforceable, the remainder of the Agreement shall continue in full force and effect.

g. Authority to Enter Agreement. The person(s) executing this Agreement on behalf of Recipient has authority to do so as an official, binding act of Recipient.

h. Conflicts. In the event of any conflict between this Security Agreement and any existing contract, purchase order, agreement or terms of service between the PSU, and Provider, the terms and conditions of this Security Agreement shall control.

SIGNATURE PAGE FOLLOWS

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

Provider:

____
[Signature, Date]

____
[Printed Name, Title]

Public School Unit:

____
[Signature, Date]

____
[Printed Name, Title]