**MEMORANDUM OF UNDERSTANDING**

**Between**

**ABC Company, Inc**

**AND**

**THE CHARLOTTE-MECKLENBURG BOARD OF EDUCATION**

This Memorandum of Understanding (“Agreement”), is entered into by ABC Company, Inc (hereinafter, Supplier) and The Charlotte-Mecklenburg Board of Education (hereinafter, “CMS”), located at 4421 Stuart Andrew Boulevard, Charlotte, North Carolina, collectively referred to as “Parties” or individually referred to as a “Party.”

The purpose of this Agreement is to clarify the responsibilities of Supplier and CMS. This Agreement supplements any other agreements into which the parties may have previously entered. To the extent to which any such agreements may be inconsistent or in conflict with this Agreement, the terms of this Agreement shall prevail.

**BACKGROUND**

Provide a description of the software and/or services provided by the Supplier. For example, *Software solutions to help students engage, explore, explain and evaluate key educational concepts created by engaging, focused lessons that encouraged students to practice their knowledge, skills, and vocabulary words in a variety of ways. The software encourages students to engage in active group discussions and answer questions that engaged them in higher-order critical thinking skills using electronic devices*.

1. **COOPERATIVE RELATIONSHIP**

Supplier and CMS agree to form a cooperative relationship under this MOU for the purpose stated above. In furtherance of this agreement:

a) *List responsibilities, actions, and deliverables for each entity.*

b)

c)

1. **PURPOSE**

The, Supplier acknowledges the responsibility of the North Carolina Department of Public Instruction in maintaining statewide student data systems and protecting student data under North Carolina General Statute 115C, Article 29. The Supplier requests access to certain SCHOOL SYSTEM DATA maintained by NCDPI and the PSU for the purpose of providing services. This MOU sets forth the terms and conditions for granting such access, ensuring that the student data is used and stored appropriately and in compliance with all applicable federal, state, and local laws, regulations, and policies. The Vendor shall receive fields and data as described in Exhibit A.

1. **DEFINITIONS**
	1. “ANONYMIZED DATA” means data that has been sanitized with the intent of privacy protection. ANONYMIZED DATA has had personally identifiable information removed so that people whom the data describe remain anonymous. It is a process of de-identification which produces data where individual records cannot be linked back to an original student record system or to other individual records from the same source, because they do not include a record code needed to link the records.
	2. “DE-IDENTIFIED DATA” means data that have undergone a process to remove or obscure any personally identifiable information in a way that minimizes the risk of unintended disclosure of the identity of individuals and information about them.
	3. “MOBILE DEVICE” means laptop computers, tablets, smart phones, or any other portable computing device.
	4. “PORTABLE STORAGE MEDIUM” – means portable memory devices, including flash or thumb drives, portable hard drives, or other portable electronic devices with the ability to store data.
	5. “SCHOOL SYSTEM” means The Charlotte-Mecklenburg Board of Education or CMS
	6. “SCHOOL SYSTEM DATA” means all confidential student and employee records or confidential student record information that contains personally identifiable student records and any other non-public student information, including but not limited to student data, metadata and user content. This includes STUDENT DATA and STAFF DATA.
	7. “PUBLIC SCHOOL UNIT” or “PSU” means The Charlotte-Mecklenburg Board of Education or CMS
	8. “SECURITY BREACH” – means an event in which SCHOOL SYSTEM DATA is exposed to unauthorized disclosure, access, alteration, destruction or use.
	9. “STUDENT DATA” – is defined as personally identifiable information or material in any media or format that is any of the following: (See Exhibit A)
		* 1. Created by or provided to Supplier by a student, or the student's parent or legal guardian, in the course of the student's, parent's, or legal guardian's use of Supplier’s site, service, or application for K-12 school purposes.
			2. Created by or provided to Supplier by an employee or agent of CMS for K-12 school purposes.
			3. Gathered by Supplier through the operation of a site, service, or application for K-12 school purposes and personally identifies a student, including, but not limited to, the data elements in Exhibit A – Student Data:
	10. “STAFF DATA” - is defined as personally identifiable information or material in any media format that is any of the following:
		* 1. Created by or provided to Supplier by an employee or agent of CMS through use of Supplier’s site, service, or application.
			2. Gathered by Supplier through the operation of a site, service, or application.
2. **ACCESS, CONTROL AND AUTHORIZATION**
3. Supplier agrees to protect and maintain the security of SCHOOL SYSTEM DATA with commercially reasonable security measures.
4. CMS is providing STUDENT DATA pursuant to the FERPA “school official” exception.
5. CMS is providing consent on behalf of parents for students less than 13 years of age as provided for by Children’s Online Privacy Protection Act (COPPA). Supplier agrees to provide CMS with full notice of collection, use, and disclosure data practices.
6. Supplier shall not authorize access to SCHOOL SYSTEM DATA to any of its agents, affiliates, contractors and subcontractors, or to any auditor, unless such agent, affiliate, contractor, subcontractor or auditor has entered into a written confidentiality agreement with Supplier agreeing to protect the confidentiality and security of such SCHOOL SYSTEM DATA. Such written confidentiality agreement shall be made available for inspection, upon demand, to CMS.
7. Supplier shall not permit unauthorized access to SCHOOL SYSTEM DATA to any individual or entity at any time.
8. Supplier shall not provide any SCHOOL SYSTEM DATA or any portion thereof to any person, party or organization ineligible to receive student records and/or student record data and information protected by FERPA, federal regulation, state law or regulation or so prohibited from receiving SCHOOL SYSTEM DATA or any portion thereof.
9. Supplier shall at all times be limited to functions of the PSU that could otherwise be provided by a school official and which the PSU is “outsourcing” to the Supplier pursuant to 34 CFR 99.31(a)(1)(B). The Supplier agrees to use the SCHOOL SYSTEM DATA for no other purpose than those identified in this Agreement. This Agreement does not convey ownership of Shared Data to the Supplier
10. Supplier or any authorized subcontractor while in the possession, custody, or control of any SCHOOL SYSTEM DATA shall insure it will 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 Supplier 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.
11. Acceptable Use - Supplier is prohibited from mining SCHOOL SYSTEM DATA for any purposes other than those agreed to in writing by CMS. 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
12. **CONFIDENTIALITY**
13. All SCHOOL SYSTEM DATA transmitted between CMS and Supplier will be protected using a cryptographic algorithm of sufficient cryptographic strength to maintain confidentiality and prevent unauthorized disclosure.
14. All STUDENT DATA, DE-IDENTIFIED DATA, ANONYMIZED DATA, or other information provided by CMS or collected by Supplier is considered confidential under this Agreement as well as under The Family Educational Rights and Privacy Act (FERPA), and any other federal or state regulations pertaining to students’ education records. To the extent that Supplier has access to any personally identifiable information from students’ education records, Supplier agrees that it shall not use such information except for the legitimate educational purpose of providing services pursuant to this Agreement and that it shall not re-disclose this information to any other party for any reason. In addition to complying with all applicable laws concerning the privacy of student records, Supplier staff will keep confidential all CMS student record information as defined Supplier privacy policy which can be found on the following website: htttp://www.somecompany.com/privacy-policy.
15. Supplier shall not sell or license STUDENT DATA, DE-IDENTIFIED DATA, ANONYMIZED DATA, or other information provided by CMS to any other party.
16. Supplier staff will comply with all applicable federal and state regulations governing the student records, including but not limited to Family Educational Rights and Privacy Act (FERPA), Protection of Pupil Rights Amendment (PPRA), the Children’s Online Privacy Protection Act (COPPA) and their North Carolina counterparts.
17. Supplier staff will sign statements in which they agree to keep confidential all CMS student record information. Supplier staff agree to comply with all applicable federal and state regulations governing the student records, including FERPA.
18. Supplier will not permit STUDENT DATA or any other confidential information related to the performance of the contracted service, site or application to be stored on any MOBILE DEVICE or PORTABLE STORAGE MEDIUM unless it is being used in connection with Supplier’s backup and recovery procedures and/or encrypted.
19. Supplier may use ANONYMIZED DATA for product development or research.
20. In the event of any unauthorized use or disclosure, Supplier will notify CMS’s Project Coordinator within twenty-four hours after the identification of a SECURITY BREACH. Supplier shall not provide details of the SECURITY BREACH to any other entity except as required by federal or state law. The Vendor shall cooperate with CMS and take such reasonable commercial steps as are directed by CMS to assist in the investigation, mitigation and remediation of each such Data Breach. Supplier agrees to provide CMS with a description of the breach, the type of data that was the subject of the breach, and other information CMS may request concerning individuals and data potentially involved.
21. Supplier will notify CMS’s Project Coordinator in writing of any material change to Supplier’s privacy policy which is found on the following website: htttp://www.somecompany.com/privacy-policy.
22. **GENERAL PROVISIONS**
23. CMS’s Project Coordinator - The project coordinator for CMS is CMS Project Coordinator (“CMS’s Project Coordinator”). CMS’s Project Coordinator shall serve as CMS’s representative in connection with this Agreement. CMS may designate a different staff person to serve as project coordinator and agrees to promptly notify Supplier’s Project Coordinator should that occur.
24. Supplier Project Coordinator - The project coordinator for Supplier shall serve as Supplier’s representative in connection with this Agreement. Supplier may designate a different staff person to serve as project coordinator and agrees to promptly notify CMS’s representative should that occur.
25. Modification – The terms of this agreement may be modified only through mutual written consent between both parties.
26. Ownership – All data provided by CMS to Supplier and any data collected by Supplier through use of the software by CMS employees or students is the sole property of CMS and will remain the property of CMS after termination of this agreement.
27. Marketing & Advertising - In no event will Supplier use any of the SCHOOL SYSTEM 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 PSU, without the express written consent of the PSU.
28. Termination - This Agreement may be terminated by either Party for any reason by giving written notice of termination to the other Party at their current office address at least thirty (30) days prior to the date of termination specified by the terminating Party in such notice. Supplier will return all personably identifiable student information or allow CMS to download this data upon termination of this agreement. Supplier will securely delete any copies still in its possession including archives and/or backups, upon termination of this agreement.
29. Compliance - Supplier agrees to comply with all applicable laws and regulations in all respects. For purposes of this 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 Agreement may be construed to allow the Supplier to maintain, use, or disclose any Shared Data in a manner inconsistent with any applicable law, regulation, or policy.
30. Indemnification - Supplier shall indemnify, protect, defend and hold CMS, its board of directors, officers, employees, contractors and volunteers harmless from and against any and all losses in connection with injury (including death) or damage to any person, property, or business sustained to the extent resulting from negligence or willful misconduct of Supplier, its agents, contractors, employees and licensees.
31. Expenses - Any expenses related to the provision of services incurred by Supplier shall be the sole responsibility of Supplier.
32. Independent Entities - The provisions of this Agreement are not intended to create and shall not be interpreted to create a joint venture, a partnership or any similar relationship between the parties. No officer, manager, director, employee, agent, affiliate or contractor of any contractor shall be deemed to be an officer, manager, director, employee, agent, contractor or sub-contractor of CMS. No contractor will have any right, power or authority, express or implied, to bind any other contractor.
33. Assignment of Rights – Neither this Agreement, nor any rights, duties, nor obligations described herein shall be assigned by Supplier without the prior express written consent of the PSU.
34. Security Measures – Supplier shall implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information and protect that covered information from unauthorized access, destruction, use, modification, or disclosure.
35. Data Destruction - Supplier shall delete a student’s covered information within 45 days if CMS requests deletion of covered information under the control of CMS, or CMS notifies the Supplier of completion of services with Supplier, unless a student who is at least 13 years of age, a parent, or a guardian, provides express written consent given in response to clear and conspicuous notice to the maintenance of covered information.
36. Right to Inspect and Correct – A parent, legal guardian, or student who has reached 18 years of age may review the student’s education records. Supplier, in conjunction with the school, will provide accommodations that will allow the inspection of these education records when CMS is presented a written request. A parent, legal guardian, or student who has reached 18 years of age may request the correction of erroneous information maintained by Supplier by providing a written request to CMS. Supplier, at the direction of CMS, will make reasonable efforts to correct the erroneous information.
37. Authority to Enter Agreement – The person(s) executing this Agreement on behalf of Supplier has authority to do so as an official, binding act of Supplier.
38. 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
39. **REQUIRED DOCUMENTATION**
40. Provider agrees to provide the PSU with a security self-assessment (VRAR) annually and in the event of any significant changes to the information required in the VRAR. The VRAR may be downloaded from https://it.nc.gov/documents/vendor-readiness-assessment-report
41. **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>. In the event that the Supplier does not currently comply with all elements of the Information Security Manual, the Supplier shall present a roadmap for implementation of all required controls. The PSU, at their sole discretion, may request additional documentation including:

1. A credentialed vulnerability scan of the Supplier’s 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.
2. 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.
3. A third-party conducted assessment report such as the Federal Risk and Authorization Management Program (FedRAMP) authorization, SOC 2 Type 2 audit, ISO 27001 certification report, or HITRUST certification report.
4. The provider shall securely share any documentation provided with CMS for evaluation and review at the request of CMS as needed to present progress towards meeting the requirements of the North Carolina Information Security Manual.
5. **FINANCIALS**

This Agreement is a non-monetary contractual agreement between the parties and is not intended to result in any direct or indirect costs to CMS.

1. **TERM**

The term of this Agreement shall be from 7/1/2020 through 6/30/2022 or until such date as this Agreement is terminated as set forth in Section 7e. This MOU may be attached to a contract as an exhibit, or it can be utilized as a standalone agreement. The parties hereto have caused this MOU to be executed by their duly authorized representatives as of the Effective Date

**[Signatures appear on the following page]**

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the day and year written above.

|  |  |
| --- | --- |
| **THE CHARLOTTE-MECKLENBURG BOARD OF EDUCATION** | **Supplier** |
| By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Title: Deputy Superintendent | By:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Title:  |
|  |  |
| By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Title: By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Title: Superintendent (If applicable) |

**Exhibit A – Student Data**

Student Data includes, but is not limited to the following data:

1. Information in the student's educational record or electronic mail.
2. First and last name.
3. Home address of the student or student’s family.
4. Telephone number.
5. Electronic mail address.
6. Other information that allows physical or online contact.
7. Discipline records.
8. Test results.
9. Special education data.
10. Juvenile dependency records.
11. Grades.
12. Evaluations.
13. Criminal records.
14. Medical records.
15. Health records.
16. Social Security number.
17. Biometric information.
18. Disabilities.
19. Socioeconomic information.
20. Food purchases.
21. Political affiliations.
22. Religious information.
23. Text messages.
24. Documents.
25. Student identifiers.
26. Search activity
27. Photos.
28. Voice recordings.
29. Geolocation information
30. Attendance.
31. Promotion.
32. Name of the student’s parent or other family members.
33. Personal identifier, such as the student’s Social Security number or unique student identifier.
34. Other indirect identifiers, such as the student’s date of birth, place of birth, and mother’s maiden name.
35. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.