Exhibit A

Addendum to North Carolina's Data Confidentiality and Security Agreement for Online Service Providers and Public School Units (v3)

This Addendum dated _____ (the "Addendum") amends the North Carolina's Data Confidentiality and Security Agreement for Online Service Providers and Public School Units ("Security Agreement") between _____ ("Public School Unit" or "PSU") and Amplify Education, Inc. (the "Provider").

The parties are entering into the Security Agreement and the parties have agreed to amend the Security Agreement as follows:

1. Section 2, Student Records and Information is hereby deleted and replaced with the following:

   "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 personally identifiable student data or information shared by the PSU with Provider pursuant to this Agreement, including but not limited to any personally identifiable information (PII) about students, and other personally identifiable student information, including, but not limited to, student data, and user content. The Shared Data will be used by Provider for the purpose of providing educational products and services as stated in Exhibit A, including populating student data into systems subscribed to by the Public School Unit to deliver such services. Provider system generated data such as log files would not be considered Shared Data. 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."

2. The first sentence of Section 3, Compliance with Applicable Laws, Policies and Procedures is hereby deleted and replaced with the following:

   "To become or remain a recipient of the Shared Data, Provider and the PSU agree to comply with all applicable laws and regulations in all respects."

3. Section 5, Procedures for Maintenance and Security of Shared Data is hereby deleted and replaced with the following:

   "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, provided that technical

personnel may access software applications containing PSU's data for the purpose of providing customer support. 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 Shared 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 student records and PII accessed in the course of providing services to the PSU shall be subject to the confidentiality and disclosure provisions of 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 Shared 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 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 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; provided, however, that technical personnel may access software applications containing the PSU's Shared Data for the purpose of providing customer support. Provider shall not forward to any person or entity other than the contracted PSU, or as otherwise permitted herein, 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 Shared Data at rest. Personally Identifiable Information ("PII") in the Shared Data subject to FERPA shall not be emailed in plain text

or used for marketing campaigns.

e. To the extent necessary to provide the services, Provider may provide access to Shared Data to subcontractors engaged by Provider in the ordinary course of business or for purposes that are incidental or ancillary to the provision of services. No such access shall be granted except in strict compliance with the terms and conditions of this Agreement and applicable law."

4. Section 6, Required Documentation, subsection (b) is hereby deleted and replaced with the following:

   "Provider agrees to provide the PSU, upon request, results of a third-party conducted assessment reports relevant to the PSU's data such as the Federal Risk and Authorization Management Program (FedRAMP) authorization, SOC 2 Type 2 audit, ISO 27001 certification report, or HITRUST certification report applicable to the Shared Data."

5. Section 7, Additional Security Measures and Documentation is hereby deleted and replaced with the following:

   "The PSU, at their sole discretion, may request additional documentation including:

   a. Upon request, the Provider shall securely share any documentation to PSU provided with the North Carolina Department of Public Instruction for evaluation and review at the request of the Department of Public Instruction.
   b. The provider also agrees to review local policies included by the PSU as an addendum to this agreement, and abide by such policies to the extent required by applicable law."

6. Section 8, Prohibition on Unauthorized Use or Disclosure of Shared Data is hereby deleted and replaced with the following:

   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, as permitted herein, or as required by law. Except as otherwise provided herein, Provider agrees not disclose any Shared Data obtained from the contracted PSU in a manner that could reasonably 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. Except as otherwise provided herein, Provider agrees and specifically warrants that it, its officers, directors, principals and employees, and any subcontractors, shall hold all confidential 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 to use student Shared Data to market additional or add-on services to parents or students within the Public School Unit, without the express written consent of the PSU.Notwithstanding, Provider may use Shared Data to recommend educational products or services to users, or to notify users about new educational product updates, features, or services.

e. In the event of any unauthorized use or disclosure of Shared Data ("Security Incident"), Provider shall report the existence of a Security Incident to the PSU without undue delay after Provider learns the PSU's Shared Data was affected by the Security Incident 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. Unauthorized disclosure shall include, but is not limited to, technical breaches, misconfigurations, invalid permissions, and any other access, all which result in a user of the system or public receiving access to Shared Data they would not otherwise be entitled to.

f. Provider shall provide a report promptly upon PSU request of the current state of the Security Incident. Provider will also provide an incident postmortem report promptly upon incident resolution. Such report shall identify, the following to the extent known:

    i. The nature of the Security Incident,

    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 Security Incident, 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 Security Incident that may be reasonably requested by NCDPI and the PSU without undue delay. To the extent the PSU determines that the Security Incident triggers third party notice requirements under applicable laws, as the owner of the Shared Data, the PSU shall be responsible for the timing and content of the notices to be sent. Except as otherwise required by law, Provider will not provide notice of the Security Incident directly to individuals whose Shared Data was affected, to regulatory agencies, or to other entities, without first providing written notice to the PSU. Provider will be responsible for, and will bear, all notification related costs arising out of or in connection with the Security Incident, subject to any limitations of liability terms contained in the Contract. For clarity and without limitation, Provider will not be responsible for costs associated with voluntary notification that is not legally required. With respect to any Security Incident that is not due to acts or omissions of Provider or its agents, Provider will reasonably cooperate in performing the activities described above, at the PSU's reasonable request and expense.

h. Provider will not release any research or publications pertaining to the Public School Unit's Shared 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."

7. Section 9, Employees, Contractors and Agents is hereby deleted and replaced with the following:

   "To the extent necessary to provide the Services as outlined herein, Provider shall ensure that all subcontractors are contractually bound to adhere to terms no less stringent than 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. 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."

8. Section 10, Investigations, is hereby deleted and replaced with the following:

"A list of Shared Data fields and types held by Provider will be made available to PSU for review and inspection upon request of the PSU. Upon request, Provider will provide the PSU with a copy of its data privacy and security statement and/or results of the most recent third party security assessment report that is relevant to the Shared Data. Notwithstanding the foregoing, as a vendor to multiple state and district customers, Provider cannot allow direct access to its systems."

9. Section 11, Term; Post-Termination is hereby deleted and replaced with the following:

   "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 Shared Data collected by the Provider in a mutually agreed format. The Transition Period may be modified in writing by the parties in a contract amendment. Upon termination and after providing the Shared Data to the PSU, if requested, the Provider shall permanently destroy or render inaccessible any Shared Data, upon request, and provide the state notice in writing of such destruction. All plugins and data sharing of PSU Shared 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 Shared 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 ninety (90) days after the effective date of the termination or expiration of this Agreement. This section shall survive the expiration or earlier termination of this Agreement."

10. Section 12, Breach and Default; Indemnification; Remedies is hereby deleted and replaced with the following:

    a. "In the event of a Security Incident, or, if the PSU determines, in their sole discretion, that Shared Data 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. Subject to the limitation of liability in the Contract, 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 third-party claims, actions, demands, costs, damages, losses, and/or expenses of any kind whatsoever proximately resulting from any Security Breach by Provider or its subcontractor(s).

c. Subject to the limitation of liability in the Contract, in the event of a Security Incident in the North Carolina Student Information System (NCSIS) determined to be caused by the actions of the Provider, the Provider shall reimburse the NCDPA for any and all reasonable costs and expenses that the NCDPI incurs in investigating and remediating the Security Incident to the extent such investigation or remediation is required by applicable law. For clarity and without limitation, Provider will not be responsible for costs associated with voluntary notification, investigation, or remediation that is not legally required.

d. 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."

11. Section 14 (e), Assignment of Rights is hereby deleted and replaced with the following:

"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 unless such assignment is to an affiliate or in the event of a merger, acquisition, or reorganization, or a sale of substantially all of Amplify's assets relating to the Contract."

12. In the event of any conflict between the Security Agreement and this Addendum, the Addendum 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]