Amplify.

New York Data Privacy and Security Addendum

The purpose of this Addendum is to facilitate educational agency compliance with New York State Education Law section 2-d and regulations promulgated thereunder ("NY Education Privacy Laws"), including the requirement under section 121.2 of the regulations that each educational agency shall ensure that it has provisions in its contracts with third party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with federal and state law and the educational agency's data security and privacy policy.

This Addendum supplements Amplify's Terms and Conditions for use of Amplify products licensed by the educational agency available at https://amplify.com/customer-terms (the "Agreement").

For the purposes of this Agreement, "breach," "commercial or marketing purpose," "disclose or disclosure," "education records," "encryption," "personally identifiable information," "release," "student data," "teacher or principal data," "unauthorized disclosure or unauthorized release" will be as defined by NY Education Privacy Laws.

1. **Bill of Rights for Data Privacy and Security.** In accordance with section 121.3 of the regulations, Amplfiy hereby agrees to comply with the parents bill of rights for data privacy and security ("bill of rights") as promulgated by the educational agency. In accordance with section 121.3(c) of the regulations, see Attachment A for supplemental information to the bill of rights.

2. **Data Security and Privacy Plan.** In accordance with Section 121.6 of the regulations, see Attachment B for Amplify's data security and privacy plan.

3. **Third Party Contractor Compliance.** In accordance with Section 121.9 of the regulations, Amplify as a third-party contractor that will receive student data or teacher or principal data, represents and covenants that Amplify will:
    - (1) adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework;
    - (2) comply with the data security and privacy policy of the educational agency with whom it contracts; Education Law § 2-d; and this Part 121;
    - (3) limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
    - (4) not use the personally identifiable information for any purpose not explicitly authorized in its contract;
    - (5) not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student: (i) except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or (ii) unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the

information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

- (6) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
- (7) use encryption to protect personally identifiable information in its custody while in motion or at rest; and
- (8) not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;
- Where Amplify engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on Amplify by state and federal law and this Agreement shall apply to the subcontractor.

4. **Reports and Notifications of Breach and Unauthorized Release.** In accordance with section 121.10 of the regulations, Amplify will:
   - promptly notify the educational agency of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach;
   - cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.
   - where a breach or unauthorized release is attributed to Amplify, Amplify shall pay for or promptly reimburse the educational agency for the full cost of such notification. In compliance with this section, notifications shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include: a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate; and contact information for representatives who can assist parents or eligible students that have additional questions.

5. **General.**
   - The laws of the State of New York shall govern the rights and duties of Amplify and the educational agency.
   - If any provision of the contract or the application of the contract is held invalid by a court of competent jurisdiction, the invalidity does not affect other provisions or applications of the contract which can be given effect without the invalid provision or application.
   - This Agreement controls over any inconsistent terms or conditions contained within any other agreement entered into by the parties concerning student, teacher and principal data.

ACKNOWLEDGED AND ACCEPTED:

BY: _____

Name: Catherine MacKay

Title: President and Chief Operating Officer

ATTACHMENT A

SUPPLEMENTAL INFORMATION FOR THE BILL OF RIGHTS

1. *The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract:*

   The purposes for which Amplify will use student, teacher, or principal data are described in Amplify's Customer Privacy Policy, available at https://amplify.com/customer-privacy/.

2. *How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d):*

   Amplify requires all subcontractors or other authorized persons with access to student, teacher, or principal data to agree in writing to abide by all applicable state and federal laws and regulations. Additionally, as between Amplify and the educational agency, Amplify takes full responsibility for the actions of any such parties.

3. *The duration of the contract, including the contract's expiration date and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed):*

   The Agreement will last for the time period described in the applicable purchasing document, unless earlier terminated in accordance with the Agreement. Student, teacher, or principal data will be returned or destroyed in accordance with whichever is the sooner of 1) the period necessary to fulfill the purposes outlined in Amplify's Privacy Policy and the Agreement, 2) applicable state and federal laws and regulations, or 3) the educational agency's option and direction.

4. *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:*

   A parent, student, eligible student, teacher or principal may contact the education agency directly to discuss the correction of any such erroneous information. If Amplify receives a request to review student data in Amplify's possession directly from such a party, Amplify agrees to refer that individual to the educational agency and to notify the educational agency within a reasonable time of receiving such a request. Amplify agrees to work cooperatively with the education agency to permit a parent, student, eligible student, teacher or principal to review student, teacher, or principal data that has been shared with Amplify and correct any erroneous information therein.

5. *Where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated:*

Amplify leverages Amazon Web Services (AWS) as its cloud hosting provider. Further information regarding Amplify's security program can be found on Amplify's Information Security page at https://amplify.com/security.

6. *Address how the data will be protected using encryption while in motion and at rest:*

   In transit: Amplify encrypts all student personal information in transit over public connections, using Transport Layer Security (TLS), commonly known as SSL, using industry-standard ciphers, algorithms, and key sizes.

   At rest: Amplify encrypts student personal information at rest using the industry-standard AES-256 encryption algorithm.

ATTACHMENT B

DATA SECURITY AND PRIVACY PLAN

In accordance with Section 121.6 of the regulations, the following is Amplify's data security and privacy plan:

1. *Outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy:*

   Amplify's privacy policy, available at amplify.com/customer-privacy/, outlines how Amplify's practices enable its customers to control use, access, sharing and retention of personal information in compliance with FERPA and other applicable privacy laws and regulations. Upon request, Amplify will also certify compliance with the educational agency's data security and privacy policy.

2. *Specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract:*

   Administrative, operational and technical safeguards and practices to protect PII under the Agreement are described in Amplify's Information Security page at https://amplify.com/security.

3. *Demonstrate that it complies with the requirements of Section 121.3(c) of this Part 121:*

   The supplemental information required by Section 121.3(c) of this Part 121 are attached to this Addendum as Attachment A.

4. *Specify how officers or employees of the third-party contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access:*

   Amplify has a comprehensive information security training program that all employees and individuals with access to Amplify systems undergo upon initial hire or engagement, with an annual refresher training. We also provide information security training for specific departments based on role.

5. *Specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected:*

   Amplify may use independent contractors engaged by Amplify in the ordinary course of business or for purposes that are incidental or ancillary to the provision of services under the Agreement. Amplify requires all subcontractors with access to student, teacher, or principal data to agree in writing to abide by all applicable state and federal laws and regulations. Additionally, as between Amplify and the educational agency, Amplify takes full responsibility for the actions of any such parties.

6. *Specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency:*

   If there has been an unauthorized release, disclosure or acquisition of the educational agency's student, teacher, or principal data, Amplify will notify the educational agency in accordance with applicable laws and regulations. Such notification will include the following steps: Amplify will notify the educational agency after Amplify determines that the educational agency's student, teacher, or principal data were released, disclosed, or acquired without authorization, (a "Security Incident"), without unreasonable delay, subject to applicable law and authorization of law enforcement personnel, if applicable. To the extent known, Amplify will identify in such a notification the following: (i) the nature of the Security Incident, (ii) the steps Amplify has executed to investigate the Security Incident, (iii) the type(s) of personally identifiable information that was subject to the unauthorized disclosure, release, or acquisition, (iv) the cause of the Security Incident, if known, (v) the actions Amplify has done or will do to remediate any deleterious effect of the Security Incident, and (vi) the corrective action Amplify has taken or will take to prevent a future Security Incident.

7. *Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.*

   Upon the termination or expiration of the Agreement and upon the educational agency's request, student, teacher, or principal data will be returned, transitioned, and/or destroyed in accordance with 1) Amplify's Privacy Policy and the Agreement, 2) applicable state and federal laws and regulations, and 3) in accordance with the educational agency's direction.