Supplemental Information for Agreement with Amplify Education, Inc. (hereinafter "Third-party Contractor"): For purposes of further ensuring confidentiality and security of personally identifiable student data, each contract ("Agreement") the Mineola Union Free School District (the "District") enters into with a third-party contractor (the "Third-party Contractor") shall include a Data Security and Privacy Plan that includes a signed copy of the District's Parents' Bill of Rights and in which Plan the Third-party Contractor agrees to abide by the District's Parents' Bill of Rights and to comply with the following:

1) **Exclusive Purposes for which Student Data Will Be Used.** Use of Personally Identifiable Information ("PII") under the Agreement will be limited to that necessary for the Third-party Contractor to perform the duties outlined in the Agreement and the services associated with that function. The Third-party Contractor further agrees that no PII will be sold or used for marketing or commercial purposes.

2) **Protective Measures Regarding Third Parties.** The Third-party Contractor will ensure that any subcontractor or other person or entity with whom the Contractor shares personally identifiable student data and/or teacher or principal data, if applicable, agrees to abide by applicable state and federal law, including New York Education Law Section 2-d, and the Family Educational Rights and Privacy Act ("FERPA"). In addition, the Third-party Contractor will ensure that each subcontractor, person or entity with whom the Third-party Contractor shares personally identifiable student data and/or teacher or principal data will abide by terms and conditions at minimum as protective as those outlined in this Data Security and Privacy Plan.

3) **Expiration of Agreement.** Absent renewal, the Agreement expires annually on June 30th. If the District does not renew the Agreement past June 30th of the contractual year, all personally identifiable student data shall be deleted, within 90 days, in accordance with the National Institute of Standards and Technology (NIST) standard 800-88. The Third-party Contractor will ensure, at the sole discretion of and upon request from the District, that all student data are returned to the District or provide confirmation to the District that the personally identifiable student data in its possession has been securely destroyed. Third-party Contractor shall ensure that any personally identifiable student data it retains after 90 days is data it is required to retain by law and retention is secured in accordance with NIST and/or HIPPA standards.

4) **Challenge to Accuracy of Data.** A parent, student, teacher or principal can challenge the accuracy of the Data received or generated by the Third-party Contractor in writing addressed to Whittney Smith, Ed.D., Director of Instructional Technology and Assessment, Mineola Union Free School District, 2400 Jericho Turnpike, Garden City Park, New York 11040.

5) **Storage of Data.** Personally Identifiable student data shall be stored in a secure data center using monitoring of the access doors, fire and security monitoring,

system health and intrusion monitoring, data backups and retentions. Data storage and access shall comply with the Advanced Encryption Standard (AES) with minimum of 128 bit key encryption or better.

6) **Breach of Personally Identifiable Information.** The Third-party Contractor must notify the District of any breach or unauthorized release of PII within seven (7) calendar days of any such breach or Third-party Contractor's knowledge of such breach. The Third-party Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of PII that is attributable to the Third-party Contractor, its subcontractors, and/or assignees to the extent such notice is required by applicable law.

MINEOLA UNION FREE SCHOOL DISTRICT	Amplify Education, Inc.
By: Cheryl Lampasona	By: Catherine Mackay
Name: Cheryl Lampasona	Name: Catherine Mackay
Title: President, Board of Education	Title: President and COO

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.