EXHIBIT B
The New York Addendum

This New York Addendum ("Addendum") is entered into between Apple and Mineola UFSD. This Addendum is a part of the Apple School Manager Agreement executed pursuant thereto by Institution and Apple (the "Agreement"). All capitalized terms used in this document but not defined shall have the meaning set forth in the Agreement. To the extent of any conflict or inconsistency between this Addendum and the terms of the Agreement, this Addendum will govern. Apple's obligations under this Addendum are in addition to, and not in lieu of, its obligations in the rest of the Agreement.

1. In compliance with New York Education Law §2-d, Apple hereby assures and warrants it shall:

   a. Limit internal access to Personal Data to those individuals determined to have legitimate educational interests in such access;

   b. Not use Personal Data for any other purposes than those explicitly authorized in the Agreement;

   c. With the exception of Apple Personnel and representatives, and personnel of Apple Service Providers carrying out their obligations pursuant to this Agreement, not disclose Personal Data to any other party without the prior written consent of the parent or eligible student, unless (i) otherwise permitted by this Agreement or (ii) required by statute or court order, in which case Apple will provide notice to You prior to disclosure, unless providing such notice is expressly prohibited by statute or court order;

   d. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Personal Data in its custody; and

   e. Use encryption technology and other commercially reasonable means (such as firewalls and password protection) to provide reasonable protection for Personal Data from unauthorized disclosure.

2. Apple's protection of Personal Data reflects the Institution's Parents Bill of Rights, a copy of which is attached hereto and incorporated into the Agreement as Exhibit C.

3. Apple will take appropriate steps to ensure compliance with security procedures by its officers, employees, and Apple Service Providers who will have access to Personal Data, including the provision of appropriate training on applicable laws governing confidentiality. Apple shall ensure that any persons authorized to process Personal Data comply with applicable laws regarding the confidentiality and security of Personal Data with regards to the Service.

4. Upon termination of the Agreement without renewal, Apple shall, if requested by Institution, assist Institution in exporting all electronically stored Personal Data previously received back to Institution. Thereafter, Apple shall promptly and securely delete and/or dispose of Personal Data remaining in the possession of Apple or Apple Service Providers.

5. Personal Data shall not be sold or released for any commercial purposes, nor shall it be sold or used for marketing purposes by Apple or Apple Service Providers.

6. As stated in Section 3C of the Agreement, Apple will (i) notify Institution, without undue delay and as required by law, if Apple becomes aware that there has been a Data Incident; and (ii) take reasonable steps to minimize harm and secure the Personal Data. In the event that Institution is legally obligated to notify a parent, eligible student, teacher or principal of a Data Incident due to the unauthorized release of Personal Data by Apple or Apple Service Providers, Apple shall promptly reimburse the Institution for the reasonable and necessary costs of such notification.
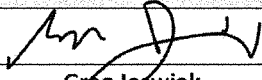
EXHIBIT C-1

Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to your school. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	
[Printed Name]	Greg Joswiak
[Title]	**Senior Vice President Worldwide Marketing**
Date:	**March 10, 2021**

EXHIBIT C-2

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Apple
Description of the purpose(s) for which Contractor will receive/access PII	To provide the Apple School Manager Service to Institution
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date : Upon agreement by Institution Contract End Date : Upon termination by Institution or Apple
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary,

	the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☒ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: As set forth in the Agreement between Apple and the Institution, including Section 3 of such Agreement.
Encryption	Data will be encrypted while in motion and at rest.