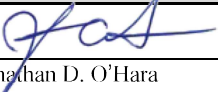


EXHIBIT B - SUPPLEMENTAL INFORMATION FOR THIRD-PARTY CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

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:	Frontline Technologies Group, LLC d/b/a Frontline Education
Description of the purpose(s) for which Contractor will receive/access PII:	* Frontline Education collects personally identifiable information (PII) on individuals including administrators, educators, students, and other as outlined in the Frontline Technologies Group LLC Privacy Policy which is available at https://www.frontlineeducation.com/about/commitment-to-security/. * Frontline Education will only use PII as specifically permitted in agreements entered with customers. Specifically, PII is used for the provision of services and tracking of information across Frontline products and platforms. * Frontline Education may use de-identified, anonymized and aggregated data for various purposes including enhancing the customer experience and refining and developing additional products and services.
Type of PII that Contractor will receive/access:	Check all that apply: XStudent PII ☐ APPR Data
Contract Term:	Contract Start Date: 7 / 1 / 2 0 2 6 _____ Contract End Date: 6 / 3 0 / 2 0 2 7 _____
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. XContractor 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 as the data is maintained by Frontline. - Securely delete and destroy data. Backup files made in the normal course of business may be retained by Contractor's data retention policy, for regulatory compliance.
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. XUsing Contractor owned and hosted solution ☐ Other (describe below):

	Frontline hosts its solutions within Amazon AWS and SunGard Availability Services Data Center(s) in a secured hybrid hosting model and maintains complete administrative control of customer data within these hosting environments. Frontline Education encrypts data within our production networks using FIPS 140-2 compliant encryption standards. All sensitive data is encrypted at rest across all storage devices using Full Disk Encryption and all database backups are AES-256 encrypted. Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: • Frontline encrypts data within its production networks using FIPS 140-2 compliant encryption standards. All sensitive data is encrypted at rest across all storage devices using Full Disk Encryption and all database backups are AES-256 encrypted. • Frontline secures all sensitive data in transit using strong encryption protocols to encrypt all traffic including use of TLS 1.2 protocols, and SHA2 signatures. • Frontline adheres to the principles of least privilege and role-based permissions when provisioning access ensuring workers are only authorized to access data as a requirement of their job function. All production access is reviewed annually, at a minimum.
Encryption:	Data will be encrypted while in motion and at rest.

CONTRACTOR	
Signature:	
Printed Name:	Jonathan D. O'Hara
Title:	VP, Controller
Date:	9/14/2026

**EXHIBIT B - SUPPLEMENTAL INFORMATION FOR THIRD-PARTY 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:	Curriculum Associates, LLC
Description of the purpose(s) for which Contractor will receive/access PII:	License to access and use Contractor's educational software
Type of PII that Contractor will receive/access:	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term:	Contract Start Date: <u>July 1, 2026</u> Contract End Date: <u>June 30, 2027</u>
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. (CA does not use subcontractors to support individual contracts but does utilize service providers to support the hosting, security, authentication, analytics, operation, improvement, and research related to the i-Ready Platform, as well as to support our internal business operations)
Data Transition and Secure Destruction:	Upon expiration or termination of the Contract, Contractor shall, upon the election of the EA: • Securely transfer data to EA 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 30 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 (describe below):

	Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: (i) Systems and servers are hosted in a cloud environment; (ii) our hosting provider implements network-level security measures in accordance with industry standards; (iii) we manage our own controls of the network environment; (iv) access to production servers is limited; (v) servers are configured to conduct daily updates; (vi) servers have anti-virus protection, intrusion protection, configuration control, monitoring/alerting, and automated backups; we conduct regular vulnerability testing.
Encryption:	Data will be encrypted while in motion and at rest.

CONTRACTOR	
Signature:	
Printed Name:	Kelly Sia
Title:	Chief Executive Officer
Date:	8/7/2026