APPENDIX S-1
Attachment To Parents' Bill Of Rights
For Contracts Involving Disclosure of Certain Personally Identifiable Information

Education Law §2-d, added by Ch. 56 of the Laws of 2014, requires that a Parents' Bill of Rights be attached to every contract with a third-party contractor (as defined in the law) which involves the disclosure of personally identifiable information (PII) derived from student education records ("Student Data"), or certain teacher/principal information regarding annual professional performance evaluations that is confidential pursuant to Education Law §30212-c ("APPR Data"). Each such Contract must include this completed Attachment to provide specific information about the use of such data by the Contractor.

1. Specify whether this Contract involves disclosure to the Contractor of Student Data, APPR Data, or both.

   ☒ Disclosure of Student Data

   ☐ Disclosure of APPR Data

2. Describe the exclusive purposes for which the Student Data or APPR Data will be used in the performance of this contract.

   Student demographic data will be provided to the Contractor for the purpose of its performing the following tasks for NYSED: administering and scoring assessments in English Language Arts, Mathematics, and Science and analyzing operational test results. The vendor will also be gathering student test result data in scoring students' responses to test questions and determining students' test results.

3. Identify any subcontractors or other persons/entities with whom the Contractor will share the Student Data or APPR in the performance of this Contract and describe how the Contractor will ensure that such persons/entities will abide by the data protection and security requirements of the Contract.

   Subcontractors or other entities with whom the Contractor will share data:

Bidder should specifically list in this section any/all subcontractors that will/may receive data.
No subcontractors will receive Student Data for this project.

In the event the Contractor engages a Subcontractor or otherwise shares Student Data or APPR Data with any other entity, Contractor acknowledges and agrees that before any such data is shared with a Contractor or another entity, such party must agree in writing to be bound by the confidentiality and data protection provisions set forth in this Contract including, but not limited to, the "Data Security and Privacy Plan" set forth in Appendix R. Upon termination of the agreement between the Contractor and a Subcontractor or other entity, Contractor acknowledges and agrees that it is responsible for ensuring that all Student Data or APPR Data shared by the Contractor must be returned to Contractor or otherwise destroyed as provided in Paragraph 4 of the "Data Security and Privacy Plan" set forth in Appendix R.

4. Specify the expiration date of the Contract and explain what will happen to the Student Data or APPR Data in the Contractor's possession, or the possession of any person/entity described in response to Paragraph 3, upon the expiration or earlier termination of the Contract.

   Contract expiration date: ***December 31, 2025***

   ☐ Contractor agrees to return the Student Data or APPR Data to NYSED consistent with the protocols set forth in Paragraph 4 of the "Data Security and Privacy Plan" set forth in Appendix R.

   ☒ Contractor agrees to securely destroy the Student Data or APPR Data consistent with the protocols set forth in Paragraph 4 of the "Data Security and Privacy Plan" set forth in Appendix R.

5. State whether the Contractor will be collecting any data from or pertaining to students derived from the student's education record, or pertaining to teachers or principals' annual professional performance evaluation pursuant to the Contract, and explain if and how a parent, student, eligible student (a student eighteen years or older), teacher or principal may challenge the accuracy of the Student Data or APPR data that is collected.

   ☒ Student Data
   ☐ APPR Data

   Any challenges to the accuracy of any of the Student Data or APPR Data shared pursuant to this Contract should be addressed to the school, educational agency or entity which produced, generated, or otherwise created such data.

6. Describe where the Student Data or APPR Data will be stored (in a manner that does not jeopardize data security), and the security protections taken to ensure that the data will be protected, including whether such data will be encrypted.

Bidder should detail in this section where data will be stored, what security measures will be in place, and whether electronic data is encrypted in motion and/or at rest.

Please describe where PII will be stored and the protections taken to ensure PII will be protected:

The Kite platform in Amazon Web Services (AWS)

Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:

The database supports:

- full restoration of databases including point-in-time restoration

-high-availability mode with automatic failover to a secondary database.

-Backup standards include a nightly backup with a full backup at least once per week. AWS backups are encrypted and stored using Amazon Simple Storage Service (S3), which is a secure, highly durable storage service designed for 99.999999999% durability, with multiple copies replicated in multiple data centers. Critical application data files are encrypted and also stored using S3.

-All sensitive data is encrypted at rest and all application network traffic is encrypted on the wire using secure encryption algorithms to protect sensitive data at all times.

Kite Student Portal and Educator Portal applications use the Spring Security framework to validate sessions and restrict access to features & application programming interfaces (APIs) through role based permissions, thereby ensuring that only authenticated and valid users can access data in the Student Portal and Educator Portal. Both the Student Portal and Educator Portal use Transport Layer Security (TLS) so that all calls to these applications are encrypted using modern, secure encryption algorithms, providing both privacy and data integrity, ensuring that data sent back and forth is secure and cannot be accessed by unauthorized users when transmitted over the network.

The Achievement and Assessment Institution (AAI) will maintain a secure file transfer protocol (SFTP) site for secure transmission of files between NYSED and AAI. Access to this site is limited to AAI and NYSED.