DATA PRIVACY RIDER FOR ALL CONTRACTS INVOLVING PROTECTED DATA PURSUANT TO EDUCATION LAW §2-C AND §2-D

District and Vendor agree as follows:

1. Definitions:

(1) Protected Data means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;

(2) Personally Identifiable Information (PII) means the same as defined by the regulations implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Data shall be maintained in accordance with State and Federal Law and the District's Data Security and Privacy Policy;

3. The Parties agree that the District's Parents' Bill of Rights for Data Privacy and Security are incorporated as part of this agreement, and Vendor shall comply with its terms;

4. Vendor agrees to comply with Education Law §2-d and its implementing regulations;

5. Vendor agrees that any officers or employees of Vendor, and its assignees who have access to Protected Data, have received or will receive training on federal and State law governing confidentiality of such data prior to receiving access;

6. Vendor shall:

(1) limit internal access to education records to those individuals that are determined to have legitimate educational interests;

(2) not use the education records for any other purposes than those explicitly authorized in its contract. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to a third party for marketing or commercial purposes;

(3) except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any personally identifiable information to any other party:

> (i) without the prior written consent of the parent or eligible student; or
>
> (ii) unless required by statute or court order and the party provides notice of the disclosure to the department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

(4) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;

(5) use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law §111-5;

(6) adopt technology, safeguards and practices that align with NIST Cybersecurity Framework;

(7) impose all the terms of this rider in writing where the Vendor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Data.