

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and _____ (the "Vendor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between Ulster BOCES (the "District") and the Vendor to the contrary, Vendor agrees as follows:

1. Vendor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Vendor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third-parties. Vendor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Vendor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Vendor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Children's Online Privacy Protection Act ("COPPA"), the Protection of Pupil Rights Amendment ("PPRA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"Protected Data" includes any information rendered confidential by New York State ("State") or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,

-AND-

Personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

2. Vendor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Vendor agrees to comply with District policy(ies) on data security and privacy. Vendor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Vendor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Vendor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Vendor's Data Security and Privacy Plan Requirements

3. Vendor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

- a. Outline how the Vendor will implement all State, federal, and local data security and privacy requirements over the life of the Agreement, consistent with the District's data security and privacy policy;
- b. Specify the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Vendor will receive under the contract;
- c. Demonstrate Vendor's compliance with the requirements of 8 NYCRR Part 121.3(c);
- d. Specify how officers or employees of the Vendor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and State laws governing confidentiality of such data prior to receiving access;
- e. Specify how Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
- f. Specify how Vendor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;
- g. Describe whether, how and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Vendor when the Agreement is terminated or expires.

4. Pursuant to the Plan, Vendor will:

- a. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5;
- b. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;
- c. Limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
- d. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
- e. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

- i. except for authorized representatives of Vendor such as a subcontractor or assignee to the extent they are carrying out the Agreement and in compliance with State and federal law, regulations and its Agreement with District; or
 - ii. unless required by statute or court order and Vendor has provided a notice of disclosure to the department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.
- f. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;
 - g. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
 - h. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

Vendor understands and agrees that it is responsible for submitting the above-referenced Data Security and Privacy Plan to the District prior to the start of the term of this Agreement. A copy of Vendor's Data Security and Privacy Plan is attached hereto as Exhibit "C". Further, Vendor shall sign a copy of the District's Parents Bill of Rights attached hereto as Exhibit "A".

Vendor's Supplemental Information Requirements

5. Vendor understands that, as part of the District's obligations under New York State Education Law § 2-d, Vendor is responsible for providing the District with supplemental information to be included in the District's Parents' Bill of Rights. Such supplemental information shall include:

- a. The exclusive purposes for which the student data or teacher or principal data will be used;
- b. How the Vendor will ensure that the subcontractors, persons or entities that the Vendor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
- c. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the Agreement;
- d. 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; and
- e. 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, including whether such data will be encrypted.

The supplemental information required to be provided is included as Exhibit "B" and is incorporated by reference herein and made a part of this Agreement.

6. In the event of a breach of the within confidentiality and data security and privacy standards provision and unauthorized release of student data or teacher or principal data, Vendor shall immediately notify the District and advise it as to the nature of the breach and steps Vendor has taken to minimize said breach. Said notification must be made in the most expedient way possible and without unreasonable delay but within no more than seven (7) calendar days of discovery of

the breach. Notification required hereunder shall be made in writing and must, to the extent available, include a description of the breach, date of incident, date of discovery, the types of personally identifiable information affected, the number of records affected, a description of Vendor's investigation, and contact information for Vendor's representatives who can assist the District. Notification must be sent to the District's Superintendent of Schools with a copy to the District's Data Protection Officer. Notifications required under this paragraph must be provided to the District at the following address:

SUPERINTENDENT'S NAME : _____
SCHOOL DISTRICT : _____
ADDRESS : _____
ADDRESS 2: _____
EMAIL: _____

7. In the event that Vendor fails to notify the District of a breach in accordance with Education Law § 2-d, and/or Part 121 of the Regulations of the Commissioner of Education, said failure shall be punishable by a civil penalty of the greater of five thousand dollars (\$5,000) or up to ten dollars (\$10) per student, teacher and principal whose data was released, provided that the maximum penalty imposed shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

8. Except as provided in Education Law § 2-d(6)(d), in the event Vendor violates Education Law § 2-d, said violation shall be punishable by a civil penalty of up to one thousand dollars (\$1,000). A second violation involving the same data shall be punishable by a civil penalty of up to five thousand dollars (\$5,000). Any subsequent violation involving the same data shall be punishable by a civil penalty of up to ten thousand dollars (\$10,000). Each violation shall be considered a separate violation for purposes of civil penalties and the total penalty shall not exceed the maximum penalty imposed under General Business Law § 899-aa(6)(a).

9. Vendor agrees that it will cooperate with the District and law enforcement, where necessary, in any investigations into a breach. Any costs incidental to the required cooperation or participation of the Vendor or its employees, agents, affiliates, or authorized users, as related to such investigations, will be the sole responsibility of the Vendor if such breach is attributable to the Vendor or its subcontractors.

10. Upon termination of this Agreement, Vendor shall return or, at the District's option, destroy all confidential information obtained in connection with the services provided herein and/or Protected Data. Destruction of the confidential information and/or Protected Data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. Vendor further agrees that the terms and conditions set forth herein shall survive the expiration and/or termination of this Agreement.

11. In the event Vendor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Vendor by State and federal law and Agreement shall apply to the subcontractor.

12. Where a parent or eligible student requests a service or product from Vendor and provides express consent to the use or disclosure of personally identifiable information by the third-party Vendor for purposes of providing the requested product or service, such use by the third-party Vendor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor: _____

Signature: _____

Date: _____

Printed Name: _____

Title: _____

EXHIBIT “A”

[INSERT DISTRICT'S PARENT'S BILL OF RIGHTS]

Contractor: _____

Signature: _____

Printed Name: _____

Date: _____

Title: _____

EXHIBIT “B”
Vendor’s Supplemental Information

Name of Vendor	
Description of the purpose(s) for which Vendor will receive/access PII	
Type of PII that Vendor will receive/access	Check all that apply: ☐ Student PII ☐ APPR Data
Agreement Term	Agreement Start Date: _____ Agreement End Date: _____
Subcontractor Written Agreement Requirement	Vendor will not utilize subcontractors without a written agreement that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the Vendor by State and federal laws and regulations, and the Agreement. (check applicable option): ☐ Vendor will not utilize subcontractors. ☐ Vendor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Vendor shall: • Securely transfer data to District, or a successor contractor at the District’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 District. If a correction to data is deemed necessary, the District will notify Vendor. Vendor agrees to facilitate such corrections within 21 days of receiving the District’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 Vendor 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:
Encryption	Data will be encrypted while in motion and at rest.

Contractor: _____

Signature: _____

Printed Name: _____

Date: _____

Title: _____

EXHIBIT “C”
Vendor’s Data Security & Privacy Plan

VENDOR’S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.