

**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 | Fuel Education, LLC |
| PII Declaration | <p>Does your organization/software collect student personally identifiable information (PII) or staff PII?</p> <p>Examples of student PII:</p> <ol style="list-style-type: none"> The student's name; The name of the student's parent or other family members; The address of the student or student's family; A personal identifier, such as the student's social security number, student number, or biometric record; Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name; <p>Examples of staff APPR PII:</p> <ol style="list-style-type: none"> Teacher Id, Social Security Number, Employee Number, Biometric Record Name, Mother's Maiden Name, Parent's Name Birthdate, Place of Birth, Address Gender, Race, Salary <p><input type="checkbox"/> IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.</p> |
| Description of the purpose(s) for which Contractor will receive/access PII | Provision account and classroom access for student, teachers, and district administrative staff. |
| Type of PII that Contractor will receive/access | <p>Check all that apply:</p> <p><input checked="" type="checkbox"/> Student PII</p> <p><input checked="" type="checkbox"/> APPR PII</p> |

| | |
|--|--|
| Contract Term | Contract Start Date <u>07/01/2024</u> Contract End Date <u>06/30/2025</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) <input type="radio"/> Contractor will not utilize subcontractors. <input checked="" type="radio"/> Contractor will utilize subcontractors. |
| Data Transition and Secure Destruction | Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> • 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) <input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party. <input type="checkbox"/> Using Contractor owned and hosted solution <input type="checkbox"/> 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. |

Western Suffolk BOCES - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

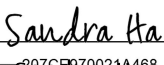
The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

| | | |
|---|--|---|
| 1 | Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract. | Stride recognizes the sensitivity of student related data stored on or passing through our E-learning solution, particularly as the platforms become part of a broader set of integrated instructional and administrative technologies. Accordingly, Stride complies with all federal, state and local statutes regarding student privacy and as provided in FERPA. If Customer is a public entity receiving federal Title I funds, Customer represents that FuelEd (Stride Learning Solutions) is a "school official" with a "legitimate educational interest" under the definitions of those terms set forth in the Customer's Family Educational Rights and Privacy Act ("FERPA") notification(s) to students and parents during the Period and Renewal Periods (if any) of any resulting Agreement, Stride agrees to develop, implement, maintain and use appropriate |
| 2 | Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII. | Stride has a legitimate educational interest for purposes of Customer disclosing to FuelEd students' education records. Regardless of whether Customer is a public entity receiving federal Title I funds, to the extent permitted by applicable law Stride or its affiliates may provide Customer with confidential information (as designated by Stride) required by Customer in writing for its internal use or reporting to regulatory authorities. Customer agrees to develop, implement, maintain and use appropriate administrative, technical or physical security measures to maintain the confidentiality of such confidential information. Terms of Use: https://www.stridelearning.com/terms-of-use.html |
| 3 | Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII. | Stride provides new workforce member computer-based security training, monthly workforce computer-based security training & education, routine email awareness email reminders, and phishing simulation exercises. |
| 4 | Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum. | Security does not control employee/contractor agreements. Please contact HR or Legal. |
| 5 | Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA. | In the event of unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information Stride will notify client following the discovery of the breach in order to be fully compliant with applicable laws and regulations. Such notifications will occur without unreasonable delay subject to the need to fully determine the scope of the breach, restore the reasonable integrity of the system or comply with law-enforcement. The notice will include to the extent possible a description of the categories of information that were reasonably believed to have been accessed or acquired by an unauthorized person and contact information that the individual may use to contact Stride for additional information about the incident. |
| 6 | Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable. | Except as required by applicable law, regulation, and/or contract, all student data is currently stored indefinitely by Stride. Stride will transition any data the district needs when requested in writing. Stride will work with the EA to identify the a secure method to transmit data that works for both parties. |
| 7 | Describe your secure destruction practices and how certification will be provided to the EA. | Except as required by applicable law, regulation, and/or contract, all student data is currently stored indefinitely by Stride. Stride will destroy or transition data to EA upon written request. |
| 8 | Outline how your data security and privacy program/practices align with the EA's applicable policies. | Stride complies with all federal, state and local statutes regarding student privacy and as provided in FERPA. If Customer is a public entity receiving federal Title I funds, Customer represents that FuelEd (Stride Learning Solutions) is a "school official" with a "legitimate educational interest" under the definitions of those terms set forth in the Customer's Family Educational Rights and Privacy Act ("FERPA") notification(s) to students and parents during the Period and Renewal Periods (if any) of any resulting Agreement. |
| 9 | Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 | Stride cybersecurity controls are aligned to the NIST CyberSecurity Framework. Policy, Controls, and Standards are aligned to the CSF. |

Western Suffolk BOCES 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: dpo@wsboces.org. (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] | DocuSigned by:  |
| [Printed Name] | Sandra Ha 297689780214488... |
| [Title] | SVP, Finance |
| Date: | 6/10/2024 |

March 12, 2024