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	SchoolAI, Inc. _____
PII Declaration	**Does your organization/software collect student personally identifiable information (PII) or staff PII?** Examples of student PII: a. The student's name; b. The name of the student's parent or other family members; c. The address of the student or student's family; d. A personal identifier, such as the student's social security number, student number, or biometric record; e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name; Examples of staff APPR PII: a. Teacher Id, Social Security Number, Employee Number, Biometric Record b. Name, Mother's Maiden Name, Parent's Name c. Birthdate, Place of Birth, Address d. Gender, Race, Salary ☐ IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT. If you collect the PII information above, please complete the remainder of this form.
Description of the purpose(s) for which Contractor will receive/access PII	To provide the SchoolAI services
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR PII

Contract Term	Contract Start Date 11/03/2026 Contract End Date 11/02/2027
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.
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 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) ☑ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor 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: Please review our trust center at: https://trust.schoolai.com/
Encryption	Data will be encrypted while in motion and at rest.

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.	See below
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See below
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.	See below
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.	See below
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.	See below
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	See below
7	Describe your secure destruction practices and how certification will be provided to the EA.	See below
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	See below
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	See below .

Additional Information (More information can be provided at the bottom 2 pages):

See below

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]	Natali Barski Signed • Sep 10, 2026
[Printed Name]	Natali Barski
[Title]	General Counsel
Date:	09/10/2026

Version: 4/30/25

Additional Information:

1. SchoolAI's platform supports SSO, role-based access, logical tenant isolation,TLS 1.3 in transit, and AES-256 at rest. Furthermore, SchoolAI conducts external penetration testing at least annually and provides personnel training within 30 days of hire and at least twice annually; monthly vulnerability scanning; continuous monitoring; sub-processors bound by written agreements; no use of Student Data for any commercial purpose to third-parties. In addition, SchoolAI conducts an annual SOC2 Type 2 independent audit. Notification to customer upon a verified security breach within the timeline required by applicable law and in no event later than 72 hours.Upon termination or expiration of thisAgreement, Student Data permanently destroyed upon written request within 90days, with no copies retained.

2. Administrative: Annually reviewed security policies; security training within 30 days of hire and at least annually; confidentiality agreements are required as a condition of employment; background checks; quarterly access reviews; vendor risk management program.● Operational: SOC 2 Type 2 with annual independent audit; monthly vulnerability scanning; annual third-party penetration testing; continuous monitoring and centralized logging; formal change management with peer code review; documented backup, BCP, and DR plans; Incident Response Plan tested annually; GCP-inherited physical controls for production infrastructure; secure media handling and disposal.● Technical: TLS 1.3 in transit andAES-256 at rest; SSO (Google,Microsoft Entra ID, ClassLink,Clever, SAML, OAuth) with MFA supported by the IdP's; 14-character minimum for passwords; multi-tenant logical isolation at database and API layers; least-privilege access with no direct ad min access to production data during normal operations; comprehensive audit logging; automated activity monitoring, vulnerability scanning, and malware detection; endpoint protection and full-disk encryption on company devices; secure SDLC incorporating OWASP Top 10. Data is not transmitted via unencrypted email.

3. Employees: All SchoolAI personnel with access to customer Student Data complete security and privacy awareness training—covering applicable confidentiality laws—prior to access, within 30 days of hire, and annually thereafter. All employees also sign NDAs and acknowledge the Information Security Program and Code of Conduct upon hire and annually.● Subcontractors (sub-processors):Subcontractors with access to customer Student Data are contractually required to comply with applicable privacy laws and maintain confidentiality agreements with their personnel.

4. Employees: As a condition of employment, employees and internal contractors must sign a confidentiality agreement, acknowledge the Information Security Program and Code of Conduct (upon hire and annually), pass role-appropriate background checks, and comply withSchoolAI's Acceptable Use Policy.Subcontractors: SchoolAI enters into written agreements with every subcontractor that accesses Student Data, and the VendorManagement Policy prohibits access until a contract with the required security controls is signed. These agreements cover information security and confidentiality obligations, incident response and breach notification timing, and training requirements for subcontractor personnel, data return/destruction upon termination, applicable geographic limits, and audit rights. The current sub-processor list is published attrust.schoolai.com; any additions, deletions, or changes will be submitted to Customer in advance via prior written notice per theDSA (including as an update to the trust page).

5.DetectionLayered detection mechanisms include continuous automated security monitoring and alerting, centralized log collection, activity monitoring, vulnerability scanning, malware detection, and a mandatory user reporting obligation.ResponseUpon identification, the InformationSecurity Manager conducts a preliminary investigation and risk assessment, assigns a severity level, and coordinates response activities with management sponsors.Activities include containment, eradication, recovery, forensic evidence preservation, and resolution. PII-specific proceduresWhere an incident involves the breach of PII, SchoolAI additionally (1) conducts an assessment to determine the extent of harm to affected parties, (2) SchoolAI takes the appropriate steps to stop the breach, (3)SchoolAI remediates any vulnerabilities that caused the breach, (4) notifies all affected parties and appropriate organizations, and(5) takes steps to mitigate harm. A post-mortem with root cause analysis and documented lessons learned follows every incident. Reporting to customer Consistent with the Data SharingAgreement, SchoolAI will notify customer upon verified breach that any Student Data has been released without authorization pursuant to the applicable timelines required by applicable law. SchoolAI will provide customer with the information necessary for customer to meet its own notification obligations underNY Ed Law §2-d.TestingThe Incident Response Plan is tested annually. Appropriate personnel complete annual incident response training.

6.TransitionCustomer will be able to export their data, as permitted by the functionality of the service during the term of the agreement

7. Upon written request by Customer following expiration and/or termination of the service agreement, SchoolAI will destroy all Student Data within ninety (90)days of said request and provide certification of same. Per the DSA, this destruction obligation does not apply to aggregated de-identified data.

8. SchoolAI's data security and privacy program is designed to meet the requirements of NY Education Law §2-d and conforms to the AICPA SOC 2 Type 2 framework, which incorporates control principles shared with other industry standards.

Additional Information: