Education Law §2-d Bill of Rights for Data Privacy and Security for Canton Central School District

Parents (includes legal guardians or persons in parental relationships) and Eligible Students (student 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and 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.
3. This right may not apply to parents of an Eligible Student.State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("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); 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 http://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. Complaints may be submitted to NYSED at http://www.nysed.gov/data-privacysecurity/report-improper-disclosure by mail to: Tim Archetko, 99 State Street Canton, NY 13617, by email to dpo@ccsdk12.org or by telephone at (315)386-8561
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.

---

[1] "Parent" means a parent, legal guardian, or person in parental relation to a student. These rights may not apply to parents of eligible students defined as a student eighteen years or older. "Eligible Student" means a student 18 years and older. [2] "Personally identifiable information," as applied to student data, means personally identifiable information as defined in section 99.3 of title thirty-four of the code of federal regulations implementing the family educational rights and privacy act, section twelve hundred thirty-two-g of title twenty of the United States code, and, as applied to teacher or principal data, means "personally

identifying information" as such term is used in subdivision ten of section three thousand twelve-c of this chapter.
[2] Information about other state and federal laws that protect student data such as the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and NY's Personal Privacy Protection Law can be found at http://www.nysed.gov/student-data-privacy/federal-laws-protect-student-data.

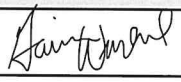
CONTRACTOR	
[Signature]	
[Printed Name]	Gavin Winkel
[Title]	Director of Revenue
Date:	12/4/24

EXHIBIT B

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	**School AI, Inc**
Description of the purpose(s) for which Contractor will receive/access PII	**Limited PII is used to customize the students' experience when connected through an LMS. This can include but not limited to data about the course, student name, and email address.**
Type of PII that Contractor will receive/access	Check all that apply: X Student PII ☐ APPR Data
Contract Term	Contract Start Date 11/11/24 Contract End Date 12/31/27
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. X 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) X 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 SchoolAI mitigates data security and privacy risks through encryption, strict access controls, data classification, and continuous monitoring. Role-based access, multi-factor authentication, and comprehensive incident response ensure only authorized access to sensitive data. Regular training and audits reinforce policy compliance, while physical security controls protect facilities and assets. Together, these layered measures uphold data integrity and confidentiality without compromising security.:
Encryption	Data will be encrypted while in motion and at rest.

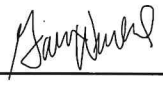
CONTRACTOR	
[Signature]	
[Printed Name]	**Gavin Winkel**
[Title]	**Director of Revenue**
Date:	12/4/24

EXHIBIT C - 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.	We enforce contract-specific data security and privacy measures through encryption, access controls, monitoring, and regular compliance audits throughout the contract term.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Safeguards include strong administrative controls, operational protocols, and technical measures such as encryption, secure access, and regular system audits to protect PII.
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.	Employees and subcontractors undergo regular training on federal and state laws governing PII confidentiality, ensuring compliance with all legal requirements.
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.	All employees and subcontractors sign binding agreements to adhere to contract requirements, with compliance closely monitored to uphold standards.
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.	A comprehensive incident response plan enables rapid identification, containment, and reporting of PII breaches, ensuring timely communication with the EA and regulatory compliance.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Data no longer needed is securely transferred to the EA using approved methods, ensuring

		data integrity and compliance during the transition process.
7	Describe your secure destruction practices and how certification will be provided to the EA.	PII is securely destroyed using certified methods, with documented certifications of destruction provided to the EA as proof of compliance.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Our data security and privacy practices are aligned with EA policies through adherence to established frameworks, continuous updates, and proactive engagement to meet EA's standards.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	SchoolAI identifies and manages data, personnel, devices, systems, and facilities through detailed inventories and classification. Assets are prioritized based on their importance to business objectives and risk strategy, with automated tools ensuring accuracy and compliance
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	SchoolAI aligns cybersecurity roles and risk management decisions with its mission, objectives, and stakeholder needs. By understanding and prioritizing organizational activities, cybersecurity efforts are tailored to protect critical operations and achieve business goals
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	SchoolAI maintains comprehensive policies, procedures, and processes to manage regulatory, legal, risk, and operational requirements. These frameworks guide cybersecurity risk management and are regularly reviewed to ensure alignment with evolving needs and compliance standards
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	SchoolAI conducts thorough risk assessments to identify and evaluate cybersecurity risks to operations, assets, reputation, and individuals. Risks are prioritized based on likelihood and impact to ensure effective mitigation and alignment with organizational objectives
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	SchoolAI defines its priorities, risk tolerances, and assumptions to guide operational risk decisions. This strategy ensures risk management efforts align with organizational goals and support informed decision-making
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	SchoolAI manages supply chain risks by establishing priorities, risk tolerances, and assumptions to guide decisions. Processes are in place to identify, assess, and mitigate risks, ensuring alignment with organizational objectives and security standards
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	SchoolAI manages identity, authentication, and access control by limiting access to authorized users, devices, and processes based on risk assessments. Role-based access, multi-factor authentication, and strict monitoring ensure security for physical and logical assets
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	SchoolAI provides regular cybersecurity training to personnel and partners, ensuring they understand their roles and responsibilities. Training aligns with policies, procedures, and agreements to maintain awareness and reduce security risks

Function	Category	Contractor Response
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	SchoolAI protects sensitive information through robust measures like data classification, encryption, and access controls based on least privilege and multi-factor authentication. Continuous monitoring, incident response planning, and regular employee training ensure data integrity and security, while physical and virtual assets are tracked and secured using automated systems. More information can be found at trust.schoolai.com
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	SchoolAI protects sensitive information through robust measures like data classification, encryption, and access controls based on least privilege and multi-factor authentication. Continuous monitoring, incident response planning, and regular employee training ensure data integrity and security, while physical and virtual assets are tracked and secured using automated systems.More information can be found at trust.schoolai.com
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	School AI has regular audits of our systems
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	SchoolAI manages technical security solutions by implementing robust access controls, encryption for data at rest and in transit, and continuous monitoring using tools like Datadog. Systems are hardened following CIS benchmarks, and regular updates ensure vulnerabilities are mitigated. Automated processes and proactive incident response measures maintain system security and resilience .
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	SchoolAI detects anomalous activity through continuous system monitoring using tools like Datadog, which identify unusual behavior and potential threats. Automated alerts and regular testing of detection processes ensure prompt identification and response to cybersecurity events
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	SchoolAI detects anomalous activity through continuous system monitoring using tools like Datadog, which identify unusual behavior and potential threats. Automated alerts and regular testing of detection processes ensure prompt identification and response to cybersecurity events
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	SchoolAI detects anomalous activity through continuous system monitoring using tools like Datadog, which identify unusual behavior and potential threats. Automated alerts and regular testing of detection processes ensure prompt identification and response to cybersecurity events
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	SchoolAI responds to cybersecurity events through a structured incident response plan that includes detection, containment, mitigation, and recovery. Response activities are coordinated across teams, with thorough analysis and documentation to incorporate lessons learned and prevent recurrence

Function	Category	Contractor Response
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	SchoolAI communicates responses to cybersecurity events by coordinating with internal teams, stakeholders, and external parties, such as law enforcement or vendors, as needed. Notifications include incident details, actions taken, and updates to ensure transparency and effective resolution
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	SchoolAI analyzes cybersecurity events by conducting thorough investigations to determine scope, impact, and root cause. This informs effective response actions, supports recovery efforts, and ensures continuous improvement through detailed documentation and lessons learned
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	SchoolAI prevents the expansion of cybersecurity events by isolating affected systems, applying patches or mitigations, and implementing containment strategies. Mitigation efforts include addressing vulnerabilities and securing impacted areas, while resolution activities focus on restoring normal operations and ensuring all remediation steps are effective
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	SchoolAI responds to cybersecurity incidents by executing a structured response plan and conducting post-incident reviews to analyze root causes and outcomes. Lessons learned are incorporated into updated policies, processes, and training to enhance future detection and response capabilities
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	SchoolAI executes and maintains recovery processes to restore systems and assets affected by cybersecurity incidents, ensuring minimal disruption. These procedures include system replication, testing, and updates to return to normal operations promptly and securely
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	SchoolAI enhances recovery planning by incorporating lessons learned from past incidents, refining processes, and updating procedures to improve resilience and effectiveness in future recovery efforts
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	SchoolAI coordinates restoration activities with internal teams and external parties, including ISPs, CSIRTs, vendors, and affected stakeholders, to ensure effective and collaborative recovery efforts