

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	NoodleTools, Inc. _____
PII Declaration	<p>Does your organization/software collect student personally identifiable information (PII) or staff PII?</p> <p>Examples of student PII:</p> <ul style="list-style-type: none"> 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; <p>Examples of staff APPR PII:</p> <ul style="list-style-type: none"> 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 <p><input type="checkbox"/> IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.</p> <p>If you collect the PII information above, please complete the remainder of this form.</p>
Description of the purpose(s) for which Contractor will receive/access PII	To provide access and basic functionality of the Noodle Tools online research platform to WS BOCES member schools.
Type of PII that Contractor will receive/access	<p>Check all that apply:</p> <p><input checked="" type="checkbox"/> Student PII</p> <p><input type="checkbox"/> APPR PII</p>



Contract Term	Contract Start Date <u>08/01/2025</u> Contract End Date <u>08/01/2030</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 checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> 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: Data security and privacy risks will be mitigated through encryption of all PII both in transit (SHA-512) and at rest (AES-256), alongside strict role-based access controls limiting data visibility to authorized personnel only. All security practices comply fully with New York Education Law 2-d, ensuring ongoing monitoring, regular security assessments, and prompt incident response protocols.
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.	We have a data privacy document for NY that applies here and can be provided upon request.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Use of up-to-date technologies, safeguards and practices that align with industry best practices including but not limited to disk encryption, file encryption, firewalls, and password protection.
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.	Training is conducted through a review and discussion of applicable federal and state privacy laws.
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.	Any 3rd-party contractors will document compliance with signed acknowledgements.
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.	We monitor data access through automated system alerts, review of audit logs, and periodic manual checks to detect unauthorized access or potential data breaches. Our breach response plan for NY details the standard steps we agree to take to report incidents. Sonarqube and owasp zap scans run for vulnerability detection.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Users can individually download any work they wish to retain.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Database deletion upon contract termination/expiration, can sign an acknowledgement if needed by EA.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	We have a data privacy document for NY that applies here and can be provided upon request.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Software dev team ISO-27001 certification enforces policies including least privilege, authentication, authorization, activity logging, isolation, and data ownership verification.


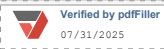
Additional Information:



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]	 
[Printed Name]	Damon Abilock
[Title]	President
Date:	07/31/2025



NoodleTools, Inc. Data Privacy and Security Plan for New York State

Last update: June 12, 2023

NoodleTools, Inc. (“Provider”) maintains this Data Security and Privacy Plan for schools in New York State, consistent with New York State Education Law 2-d Rider for Data Privacy and Security. New York State schools may purchase a license (annual subscription) to NoodleTools. NoodleTools is an online platform promoting authentic research and original writing. Students can build accurate source citations, write and organize notes, collaborate in teams, and receive in-context feedback from teachers.

The Personally Identifiable Information (“PII”) that is collected is data that is essential for providing access and user authentication into the platform. Specifically, that may include one or more of the following: email address, first name, last name, graduation year. The IP address of a user’s session is recorded. No other PII is recorded or used by the NoodleTools platform.

Provider holds all PII in compliance with all applicable provisions of federal, state and local law, including but not limited to FERPA and New York Education Law §2-d.

In accordance with New York Education Law §2-d, individuals may challenge/correct PII that is stored for a NoodleTools user. If Provider has signed a Parents Bill of Rights with the school/district, students and parents should follow the directions noted therein to request such corrections. Alternatively, a parent, student, or staff member may submit a request to support@noodletools.com. Requests are handled within 48 hours.

As required by New York State law, when a school or district terminates its NoodleTools license, all data that has been stored for that entity will be destroyed. Other circumstances that data may be destroyed are when (a) the licensee requests it or (b) the data is no longer required to provide the service to the licensee.

Provider employs industry standard security technologies to protect Data from unauthorized disclosure or acquisition by an unauthorized entity. When NoodleTools is accessed through a web browser, Secure Socket Layer (SSL) is employed to protect data from unauthorized access. Server authentication and data encryption protects data at rest and in transit, and a firewall is periodically updated according to industry standards. Periodic risk assessments are run and any security and privacy vulnerabilities are remediated in a timely manner.

Provider limits access to PII to only core owners and employees who have a specific purpose for maintaining and processing such information. Anyone given access is provided with training to protect the confidentiality of that data, covering all applicable data privacy laws and regulations.

Provider maintains and stores school/district data and PII on servers that physically reside in the United States, and will never transmit that data to any entity located outside of the United States. Provider will never provide or sell this data to any third party for any purpose. PII will never be used for any purpose other than in connection with the services provided to the school or district. PII will never be used for any form of targeted advertising.

Provider does not hire or work with subcontractors.

Provider has implemented policies and procedures addressing a potential security breach and maintains a security breach response plan. Provider will comply with all applicable federal and state laws that require notification to individuals, schools, districts or other entities in the event of a security breach.



Damon Abilock
President
NoodleTools, Inc.

NoodleTools, Inc. Breach Response Plan

Last update: June 12, 2023

In the event that Student Data is accessed or obtained by an unauthorized individual, NoodleTools, Inc. ("Provider") shall provide notification to the school or district ("Subscriber") within forty-eight (48) hours. Provider shall email a Notice of Data Breach to account contacts on record that details what happened, what Student Data was involved, and what is being done to resolve the issue. Subscriber will be given NoodleTools email and phone contact information to obtain more information.

The email will specifically include:

- A description of the breach in plain language.
- Specific Student Data that NoodleTools believes to have been compromised.
- Estimated date or date range the breach occurred.
- A description of what NoodleTools has done to protect against further data breach.
- Advice to individuals whose information has been breached.
- NoodleTools contact information to obtain further details.

Provider agrees to adhere to all requirements in applicable State and federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

Provider maintains and keeps updated a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information.



Damon Abilock
President
NoodleTools, Inc.