

## 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 NoodleTools, Inc. (the "Contractor") 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 the LINDENHURST UNION FREE SCHOOL DISTRICT (the "District") and Contractor to the contrary, Contractor agrees as follows:

Contractor 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 Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor 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. Contractor 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, Contractor 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 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 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.




Contractor 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, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor 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 Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

### **Data Security and Privacy Plan**

Contractor 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:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Contractor 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;
4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Contractor 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 educational agency;
6. Specifies whether Protected Data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

**Initial Here:** Pursuant to the Plan Contractor will:

- 
- 
- 
1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
  2. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;
  3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

**Initial Here:**

DA

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

DA

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

- a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or
- b. unless required by statute or court order and Contractor 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.

DA

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

DA

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

DA

8. 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.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

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

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of the District's Parent Bill of Rights.

**NAME OF PROVIDER: NoodleTools, Inc.**

**SIGNED BY:**  **DATED: 5/15/2025** \_\_\_\_\_

**TITLE: President** \_\_\_\_\_

## **DATA PRIVACY AND SECURITY PLAN**

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

## **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](mailto: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.