

**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).

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

<b>Contract Term</b>	Contract Start Date <u>10/24/2024</u> Contract End Date <u>10/23/2025</u>
<b>Subcontractor Written Agreement Requirement</b>	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.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> <li>• 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.</li> <li>• Securely delete and destroy data.</li> </ul>
<b>Challenges to Data Accuracy</b>	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.
<b>Secure Storage and Data Security</b>	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:
<b>Encryption</b>	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.	Contractor will ensure that it has and keeps appropriate administrative, technical, operational, and physical safeguards and practices in place through the term of the Agreement to meet all state, federal, and local data security and privacy requirements. For example, only the employees, contractors, and sub-processors who have a "need to know" have access to any PII, actually have access to the PII by instituting separate types of
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Contractor will ensure that only the employees, contractors, and sub-processors who have a "need to know" can access any PII, and only have access to the PII by instituting separate types of user-permissions on the Contractor platform back-end.
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.	Contractor shall ensure commercially reasonable efforts that all its employees, officers and Subcontractors who have access to PII have received or will receive annual training on the federal and state laws governing confidentiality of such data prior to receiving access.
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.	Contractor will ensure that all employees, contractors, and sub-contractors sign confidentiality agreements and non-disclosure agreements that limit the use of the data that is received in the course of their relationship with Contractor to the limited purpose of providing the services needed to provide the Contractor services to the EA. Contractor shall ensure that a contract is in place between it and any third party entity or agent that participates in an onward transfer of PII. The contracts specify that such PII may only be processed for limited and specified purposes consistent with the consent
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.	1. Understand the Breach 2. Fix the Breach EA. 3. Take Preventative Measures 4. Document the Breach 5. Contractor will promptly notify EA of any Breach or unauthorized release of PII in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such Breach. Contractor will cooperate with EA and law enforcement to protect the integrity of investigations into the Breach as provided in the DPA.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	It's self-service via the platform. The EA owns and controls its data at all times and may transfer the personally identifiable student data at any time.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Contractor agrees to destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, Contractor will provide EA with certification of such destruction.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor will implement the data protection and security requirements as a "third party contractor" as outlined in 8 NYCRR Part 121 and in accordance with this Contract. Contractor will also include the District's Parent's Bill of Rights and Supplemental Information to the Service Agreement. See also: <a href="https://renaissance.widen.net/view/pdf/br9e512u2u/Nearpod---Flocabulary-Terms-of-">https://renaissance.widen.net/view/pdf/br9e512u2u/Nearpod---Flocabulary-Terms-of-</a>
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	See attached Exhibit

## 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](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. (i) Complaints should be submitted to: [dpo@wsboces.org](mailto:dpo@wsboces.org). (ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-security/report-improper-disclosure](http://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](mailto: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]	Scott Johnson
[Title]	Director, Information Security
Date:	10 / 29 / 2024

March 12, 2024

Title	BOCES Data Privacy Form
File name	BOCES_DataPrivacy_20240312_.pdf
Document ID	f9299c095f9e02ea95263f442a27c5e7707e4bfd
Audit trail date format	MM / DD / YYYY
Status	● Signed

## Document History



SENT

**10 / 29 / 2024**

15:02:27 UTC

Sent for signature to Scott Johnson

(scott.johnson@renaissance.com) from amber.gish@nearpod.com

IP: 67.11.97.50



VIEWED

**10 / 29 / 2024**

15:51:56 UTC

Viewed by Scott Johnson (scott.johnson@renaissance.com)

IP: 130.41.49.36



SIGNED

**10 / 29 / 2024**

15:52:42 UTC

Signed by Scott Johnson (scott.johnson@renaissance.com)

IP: 130.41.49.36



COMPLETED

**10 / 29 / 2024**

15:52:42 UTC

The document has been completed.