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	Super Duper, Inc. dba Super Duper Publications _____
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	HearBuilder Online Subscriptions, Super Duper Digital Library, and Apps.
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR PII

Contract Term	Contract Start Date 10/16/2024 Contract End Date 10/16/2025
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: Contractor will use reasonable administrative, technical and physical safeguards that align with the NIST Cybersecurity Framework and are otherwise consistent with industry standards and best practices, including but not limited to: encryption, firewalls, and password protection as specified by the Secretary of the United States Department of HHS in any guidance issued under P.L. 111-5,
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.	Please see attached schedules A&B
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Please see attached schedules A&B
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.	Please see attached schedules A&B
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.	Please see attached schedules A&B
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.	Please see attached schedules A&B
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Please see attached schedules A&B
7	Describe your secure destruction practices and how certification will be provided to the EA.	Please see attached schedules A&B
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Please see attached schedules A&B
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Please see attached schedules A&B

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]	Abraham Webber Verified by pdfFiller 10/16/2024
[Printed Name]	Abraham Webber
[Title]	Vice President of Operations
Date:	10/16/2024

Version: 3/12/24

SCHEDULE A

Parent's Bill of Rights Supplemental Information

1) List the exclusive purposes for which the Student Data or Teacher or Principal Data will be used by the third-party contractor, as defined in the contract;

   The Contractor shall maintain Student Data for and on behalf of the District – in accordance with New York State Education Law 2-d and the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g(a)(4)(A)(ii), 1232g(b)(1) -- for the purpose of providing HearBuilder Online services (herein "Licensed Product"). The Contractor may use the Student Data to conduct collection of metrics to track student progress and performance for teacher reporting activities, including, but not limited to, longitudinal studies, alignment studies, and norming studies for the benefit of the District and/or for the collective benefit of multiple Districts, as permitted by FERPA.

2) Explain how the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the Student Data or Teacher or Principal Data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d);

   Personally identifiable information ("PII") derived from Student Data provided to the Contractor may be disclosed only to the Contractor's employees who have a legitimate educational interest in maintaining, organizing, or analyzing the data for uses authorized in their Licensed Product. PII derived from Student Data and maintained by the Contractor shall not be further disclosed by the Contractor, except as allowed by New York State Education Law 2-d and FERPA.

3) State the duration of the contract, including the contract's expiration date and a description of what will happen to the Student Data or Teacher or Principal Data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed).

   When the Agreement between the District and the Contractor expires or services are terminated, by either party, for any reason, the Contractor agrees to permanently delete all data and provide written verification confirming permanent deletion. Otherwise, all Student Data in an account is deleted automatically from the system 60 days after a Licensed Product expiration date has lapsed. Upon deletion, neither the Contractor nor the District will be able to restore deleted data.

4) State if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the Student Data or Teacher or Principal Data that is collected;

Any challenges concerning the accuracy of Student Data and/or Principal Data shall be handled directly between the District and the Parent, Student, Eligible Student, Teacher or Principal. The Contractor agrees to abide by the outcome of such challenges and make any corrections and/or changes to the applicable Student Data and/or Principal or Teacher Data as determined by the District.

5) State where the Student Data or Teacher or Principal Data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated; and explain how the data will be protected using encryption while in motion and at rest.

The Contractor takes security seriously and employs reasonable security measures and procedures designed to protect District information from unauthorized access and improper use. Only employees and trusted contractors supporting the operation of the Licensed Product have access to personal information. These individuals and entities shall be bound to protect the information appropriately. Additional security provisions include, but are not limited to:

- Sensitive data (such as passwords) are stored encrypted at rest.
- All data transfer between browser and server is encrypted via SSL.
- Student profile information is stored separately from performance data.
- Accounts are locked out after repeated, failed login attempts.
- Accounts are automatically logged out after 20 minutes of inactivity.
- Applications and data are stored and secured on separate, dedicated servers behind firewalls at secure facilities.
- Developer access is restricted and logged via secure VPN connections.
- Network is tested daily by Halo Security (formerly McAfee Secure) for weaknesses.

The Contractor's servers that store personal information are maintained in a physical environment that utilizes industry-standard security measures by Rackspace, Inc., the Contractor's web hosting company. Personal information is stored in password-controlled servers with limited access. When the District enters sensitive information (such as login credentials) we encrypt the transmission of that information using secure socket layer technology (SSL).

The Contractor's web hosting company, Rackspace, Inc. complies with New York State Education Law 2-d, this Agreement, and provides a number of additional security measures. These include, but are not limited to, the following:

- Performs pre-employment background screening on all employees with access to Super Duper, Inc. data.
- Restricts administrative access codes specific to the Contractor's accounts and all activity is logged.
- Agrees to maintain physical, technical, and administrative safeguards defined in the Payment Card Industry-Data Security Standard (PCI-DSS).
- Staffs all data centers 24/7/365 and monitored by video surveillance and viewed by onsite security force.

- Conducts routine audits and use of electronic access control system which logs access to physical facilities.
- Limits access to physical facilities to authorized individuals by proximity-based access cards and biometric hand scanners.
- Adheres to the best practice standards of ISO 27002; SSAE 16 and ISAE 3402 compliance frameworks; as well as AT 101 compliance framework. The annual SOC reports are reviewed by the Contractor and can be made available upon request.
- Reports any material breach of security which results in unauthorized access to the Contractor's data.

For more information specific to Rackspace, Inc., please consult Rackspace Inc.'s Global Security Practices found here:
https://www.rackspace.com/information/legal/securitypractices

SCHEDULE B

Data Security and Privacy

1) Outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy;

   Super Duper, Inc. is strongly committed to the privacy of Customers and Students, particularly the privacy of children. Super Duper, Inc. complies with the requirements of the Children' s Online Privacy Protection Act of 1998 (COPPA), the Children' s Internet Protection Act (CIPA), and FERPA regarding the information collected and maintained by Super Duper, Inc. Accordingly, we will not collect, use or disclose personal information covered by COPPA, CIPA, and FERPA except in compliance with the respective requirements of each of these statutes and their associated regulations.

   With respect to CIPA, Super Duper, Inc.'s Licensed Product is self-contained and does not provide links to external resources or chat rooms. Moreover, HearBuilder Online does not contain any offensive or inappropriate matter. As a result, any school or clinic that uses HearBuilder Online will be fully compliant with CIPA.

   We will also comply with all other applicable laws which govern the information maintained by Super Duper, Inc.

2) Specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract;

   How Super Duper, Inc. Complies

   - Any sensitive online information is transmitted over secure, encrypted channels via SSL as well as other layers of encryption.
   - All Student Data is stored on secure servers utilizing encryption and firewall technology and are not publicly accessible.
   - All Student performance data is stored in a non-identifiable format.
   - Security audits are continuously performed to ensure data integrity.
   - Super Duper, Inc. does not share Student Data with any third parties. If a school requests that Student Data should be sent to a third party, Super Duper, Inc. sends the data to the school and never directly to the third party.
   - Super Duper, Inc. commits to continued employee training to ensure compliance with New York State Education Law 2-d, FERPA, and other relevant laws and regulations.

   Additional compliance requirements are detailed below.

   Super Duper, Inc. is dedicated to the privacy of children under 13 years of age. We do not process or collect from children more personal information than is needed to access services. The Customer is responsible for obtaining all parental consent necessary for collection of

personal information from children under 13. Super Duper, Inc. presumes that such consent has been obtained by Customer by virtue of the Customer having retained Super Duper, Inc. to provide its services.

Parents may review their Student' s PII by contacting the Customer. If a request is made to Super Duper, Inc., we will look to the Customer to validate the request and respond accordingly.

Super Duper, Inc. will not share any personal information about children with any third parties other than as specified in this Privacy Policy.

3) Demonstrate that it complies with the requirements of Section 121.3(c) of this Part (Bill of Rights);

Personally identifiable information ("PII") derived from Student Data provided to Super Duper, Inc. may be disclosed only to Super Duper, Inc. employees who have a legitimate educational interest in maintaining, organizing, or analyzing the data for uses authorized in their Licensed Product. PII derived from Student Data and maintained by Super Duper, Inc. shall not be further disclosed by Super Duper, Inc., except as allowed by New York State Education Law 2-d and FERPA. Super Duper, Inc. will abide by and maintain all provisions and regulations in the District's Privacy Bill of Rights for Parents and Students a copy of which has been executed and attached to this document.

4) Specify how officers or employees of the third-party 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;

Super Duper, Inc. limits access to Protected Data to authorized staff in various ways. Some of these ways include, but are not limited to:

- Super Duper, Inc. employees pass pre-employment background checks.
- Employee roles are separated and monitored logged through password-protected, secure internal network.
- Account access is tailored narrowly to specific roles to limit access to Protected Data. For example, a customer service agent may confirm a password reset request initiated by the Customer, but not able to access Student Data affiliated with said Customer.
- Super Duper, Inc. premises is accessible only through logged key-card access.
- Facilities are monitored 24/7/365 by video surveillance and monitored onsite.
- Access to Protected Data is monitored and logged.
- Super Duper, Inc. is committed to ongoing training, supervision, and assessment of employees so that staff will be trained to be New York State Education Law 2-d compliant, and demonstrate they understand the depth of their responsibilities and are committed to compliance with this law.
- Training and assessment will take place at a minimum on an annual basis and when changes, if any, occur in New York State Education Law 2-d and relevant laws.

- At a minimum, Super Duper, Inc. annually reviews its policies and procedures to stay current with federal and state laws regarding data privacy and security.
- Super Duper, Inc. also reviews these policies and procedures upon updates to New York State Education Law 2-d, FERPA, and any other relevant state or federal laws and regulations.

5) Specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

Super Duper, Inc. does not sell, rent, or lease Customer data to third parties. Super Duper, Inc. may share data with trusted partners to help promote safety and security, provide customer support, and to provide the Licensed Product. All such third parties are prohibited from using the Protected Data except to provide these services to Super Duper, Inc. and they are required to maintain the confidentiality of Customer information in compliance with New York State Education Law 2-d.

Super Duper, Inc.'s web hosting company, Rackspace, Inc. complies with New York State Education Law 2-d, this Data Security and Privacy Plan, and provides a number of additional security measures. These include, but are not limited to, the following:

- Performs pre-employment background screening on all employees with access to Super Duper, Inc. data.
- Restricts administrative access codes specific to Vendor accounts and all activity is logged.
- Agrees to maintain physical, technical, and administrative safeguards defined in the Payment Card Industry-Data Security Standard (PCI-DSS).
- Staffs all data centers 24/7 /365 and monitored by video surveillance and viewed by onsite security force.
- Conducts routine audits and use of electronic access control system which logs access to physical facilities.
- Limits access to physical facilities to authorized individuals by proximity-based access cards and biometric hand scanners.
- Adheres to the best practice standards of ISO 27002; SSAE 16 and ISAE 3402 compliance frameworks; as well as AT 101 compliance framework. The annual SOC reports are reviewed by Super Duper, Inc. and can be made available upon request.
- Reports any material breach of security which results in unauthorized access to Vendor data.

For more information specific to Rackspace, Inc., please consult Rackspace Inc. 's Global Security Practices found here:
https://www.rackspace.com/information/legal/securitypractices

6) Specify how the third-party 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;

Super Duper, Inc. takes security seriously and employs reasonable security measures and procedures designed to protect Customer information from unauthorized access and improper use. Only employees and trusted contractors supporting the operation of the Solution have access to personal information. These individuals and entities shall be bound to protect the information appropriately. Additional security provisions include, but are not limited to:

- Sensitive data (such as passwords) are stored encrypted at rest.
- All data transfer between browser and server is encrypted via SSL.
- Student profile information is stored separately from performance data.
- Accounts are locked out after repeated, failed login attempts.
- Accounts are automatically logged out after 20 minutes of inactivity.
- Applications and data are stored and secured on separate, dedicated servers behind firewalls at secure facilities.
- Developer access is restricted and logged via secure VPN connections.
- Network is tested daily Halo Security (formerly McAfee Secure) for weaknesses.

Super Duper, Inc. servers that store personal information are maintained in a physical environment that utilizes industry-standard security measures by Rackspace, Inc., Super Duper, Inc. 's web hosting company. Personal information is stored in password-controlled servers with limited access. When the Customer enters sensitive information (such as login credentials) we encrypt the transmission of that information using secure socket layer technology (SSL).

Despite our best efforts, no security measures are perfect or impenetrable. In this regard, we are not responsible for events or conditions beyond our reasonable control to the extent that they relate to or impact the obligations assumed, or commitments made, hereunder. However, in the event of any data breach or other violation caused by factors outside of our reasonable control, Super Duper, Inc. will comply with all applicable laws in this regard, including those requiring notification in the event of certain defined data breaches. Any notifications to Customers will be in accordance with New York State Education Law 2-d and other relevant laws and regulations.

In the event of a data breach, the following steps will be taken:

Step 1: Launch an investigation. This investigation should determine:

i. What data was accessed
ii. Which customers could be impacted
iii. The source of the breach
iv. Weaknesses in the security measures that allowed the breach to take place

Step 2: Take steps to seal the breach.
Step 3: Notify impacted customers promptly, clearly communicating the findings of the investigation and what measures have been implemented in Step 2.
Step 4: Communicate with customers as future preventative steps are implemented.

7) Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

Account administrators/teachers can easily modify the profiles of their students via the system's web interface at any time. Customer can request the deletion of his or her entire account's data by Super Duper, Inc. at any time. If services are terminated, by either party, for any reason, Super Duper, Inc. agrees to permanently delete all data and provide written verification confirming permanent deletion. Otherwise, all Student Data in an account is deleted automatically from the system 60 days after a Licensed Product expiration date has lapsed.

Upon deletion, neither Super Duper, Inc. nor Customer will be able to restore deleted data.

Privacy Contact lnformation

Super Duper, Inc. takes privacy issues very seriously. If you have any questions, suggestions or concerns, please contact us at:

Super Duper, Inc.
ATTN: Privacy Concerns
5201 Pelham Road
Greenville, SC 29615

Phone: 1-800-277-8737
Email: privacy@superduperinc.com