SCHEDULE E
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 Vendor 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 ESBOCES and Vendor to the contrary, Vendor agrees as follows:

Vendor 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 Vendor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Vendor 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. Vendor 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, Vendor shall have in place sufficient internal controls to ensure that ESBOCES' and/or Participants' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, CIPA, FERPA and HIPAA, 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 ESBOCES and/or a Participant. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of ESBOCES and/or its Participants as that term is defined in §99.3 of the Family Educational Rights and Privacy Act (FERPA),
>
> -AND-
>
> Personally identifiable information from the records of ESBOCES and/or its Participants 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

Vendor 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, Vendor agrees to comply with ESBOCES policy(ies) on data security and privacy. Vendor shall promptly reimburse ESBOCES and/or its Participants for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Vendor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Vendor shall return all of ESBOCES' and/or its Participants' data, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Vendor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES and/or its Participant's Protected Data, shall maintain a Data Security and Privacy Plan that includes the following elements:

1. A provision incorporating the requirements of ESBOCES' Parents' Bill of Rights for data security and privacy, to the extent that any of the provisions in the Bill of Rights applies to Vendor's possession and use of Protected Data pursuant to this Agreement.

2. An outline of how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the Vendor's policy on data security and privacy.

3. An outline of the measures taken by Vendor to secure Protected Data and to limit access to such data to authorized staff.

4. An outline of how Vendor will use "best practices" and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff.

5. An outline of how Vendor will ensure that any subcontractors, persons or entities with which Vendor will share Protected Data, if any, will abide by the requirements of Vendor's policy on data security and privacy, and the contractual obligations with respect to Protected Data set forth herein.

DATA SECURITY AND PRIVACY PLAN

Vendor's DATA SECURITY AND PRIVACY PLAN is as follows:

Vendor (hereinafter also referred to as "Super Duper Inc.") and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or Participants' (hereinafter also referred to as "Customer") Data, shall maintain a Data Security and Privacy Plan that includes the following elements:

1. A provision incorporating the requirements of Eastern Suffolk BOCES' Parents' Bill of Rights for data security and privacy, to the extent that any of the provisions in the Parents' Bill of Rights applies to Vendor's possession and use of Protected Data pursuant to this Agreement.

   Super Duper Inc. shall maintain Student Data for and on behalf of Customer – 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"). Super Duper Inc. 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 Customer and/or for the collective benefit of multiple Customers, as permitted by FERPA.

   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 Eastern Suffolk BOCES' Parents' Bill of Rights a copy of which has been executed and attached to this document.

2. An outline of how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the Agreement, consistent with the Vendor policy on data security and privacy.

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

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 publically 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.

Parental Consent

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.

Data Deletion

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.

The Children's Internet Protection Act (CIPA)
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.

3. An outline of the measures taken by Vendor to secure Protected Data and to limit access to such data to authorized staff.

Vendor Employee Protocols
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.

4. An outline of how Vendor will use "best practices" and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff.

Security Provisions
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 by 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).

Data Breaches & Additional Limitations
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.

5. An outline of how Vendor will ensure that any subcontractors, persons or entities with which Vendor will share Protected Data, if any, will abide by the requirements of Vendor's policy on data security and privacy, and the contractual obligations with respect to Protected Data set forth herein.

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

Privacy Contact Information
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

An executed copy of ESBOCES' Parent's Bill of Rights is attached hereto and incorporated herein.

PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record maintained by Eastern Suffolk BOCES.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review at: http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx, Or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Peggie Staib, Ed.D.
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
pstaib@esboces.org

Or in writing to:

Chief Privacy Officer, New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov.

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract the Agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

2. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

4. 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; and

5. 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, including whether such data will be encrypted.

Third Party Contractors are required to:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.

3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
9. Provide a signed copy of this Bill of Rights to Eastern Suffolk BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

Vendor hereby acknowledges that it is aware of and agrees to abide by the terms of this Bill of Rights. A copy of this signed document must be made a part of Vendor's data security and privacy plan.

SUPER DUPER INC.

SIGNATURE: 

NAME: M. Thomas Webber Jr.

TITLE: CEO