

NEW YORK STATE MODEL DATA PRIVACY AGREEMENT FOR EDUCATIONAL AGENCIES

JAMESTOWN CITY SCHOOL DISTRICT

and

SUPER DUPER INC.

This Data Privacy Agreement ("DPA") is by and between the Jamestown City School District ("JCSD"), an Educational Agency, and Super Duper Inc. ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable

form in which there is a low probability of assigning meaning without use of a confidential process or key.

8. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency 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.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to JCSD pursuant to an agreement through which Contractor will provide JCDS with services related to an educational technology service agreement for the use of HearBuilder ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("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); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and JCSD's policies. Education Law Section 2-d requires that Contractor provide JCSD with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. JCSD Data Security and Privacy Policy

State law and regulation requires JCSD to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with JCSD's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon request by JCSD, Contractor shall provide JCSD with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, JCSD's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to JCSD. Contractor may provide JCSD with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify JCSD and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify JCSD of the court order or subpoena in advance of compliance but in any case, provides notice to JCSD no later than the time the PII is disclosed, unless such disclosure to JCSD is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to JCSD, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to JCSD, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by JCSD for purposes of facilitating the transfer of PII to JCSD or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to JCSD.
- (b) If applicable, once the transfer of PII has been accomplished in accordance with JCSD's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies; archived copies, electronic versions; electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Contractor shall provide JCSD with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

- (a) Contractor shall promptly notify JCSD of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist JCSD. Notifications required by this section must be sent to JCSD's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify JCSD shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.
- (b) Notifications required under this paragraph must be provided to JCSD at the following address:

Chief Information Officer
Jamestown City School District
197 Martin Road
Jamestown NY 14701
DPO@jpsny.org

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with JCSD and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse JCSD for the full cost of JCSD's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by JCSD. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to JCSD's requests for access to Student Data so JCSD can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify JCSD and refer the Parent or Eligible Student to JCSD.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, JCSD is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

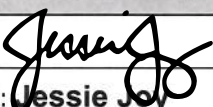
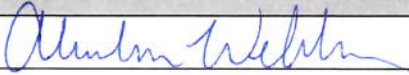
EDUCATIONAL AGENCY	CONTRACTOR
BY: 	BY: 
Name: Jessie Joy	Name: Abraham Webber
Title: Chief Information Officer	Title: Vice President of Operations
Date: 2/22/24	Date: 2/19/2024

EXHIBIT A

Education Law §2-d Bill of Rights for Data Privacy and Security Jamestown City School District

The Jamestown City School District is committed to protecting the privacy of student data and teacher and principal data. In accordance with New York Education Law §2-d and its implementing regulations, 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. Parents have 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. Parents have the right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints should be submitted in writing to the Jamestown City School District, Data Protection Officer, 197 Martin Road, Jamestown NY 14701, or by email to DPO@jpsny.org. 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. Parents will 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.

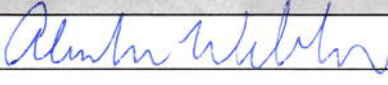
CONTRACTOR	
[Signature]	
[Printed Name]	Abraham Webber
[Title]	Vice President of Operations
Date:	2/19/2024

EXHIBIT B

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
Description of the purpose(s) for which Contractor will receive/access PII	HearBuilder Online Services
Type of PII that Contractor will receive/access	Check all that apply: ☒ Student PII ☐ APPR Data
Contract Term	Contract Start Date <u>2/19/2024</u> Contract End Date <u>2/19/2025</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) ☒ 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 JCSD'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 JCSD. If a correction to data is deemed necessary, JCSD will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving JCSD'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:
Encryption	Data will be encrypted while in motion and at rest.

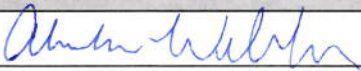
CONTRACTOR	
[Signature]	
[Printed Name]	Abraham Webber
[Title]	Vice President of Operations
Date:	2/19/2024

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

Pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations, JCSD is required to ensure that all contracts with a third-party contractor include the contractor's Data Security and Privacy Plan. **The Contractor must complete the following or provide a plan that materially addresses these requirements.**

In addition to complying with the terms of JCSD's Parents' Bill of Rights, Contractor shall protect the confidentiality, privacy and security of Protected Data received from JCSD as set forth below:

1. In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Privacy Agreement, and in a manner consistent with JCSD's data security and privacy policy, Vendor shall take the following measures to implement all state, federal, and local data security and privacy requirements over the life of the agreement:

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.

2. Contractor shall have the following administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from JCSD under this Data Privacy Agreement:

- ① Any sensitive online information is transmitted over secure, encrypted channels via SSL as well as other layers of encryption.
- ① All Student Data is stored on secure servers utilizing encryption and firewall technology and are not publicly accessible.
- ① All Student performance data is stored in a non-identifiable format.
- ① Security audits are continuously performed to ensure data integrity.
- ① 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.
- ① 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.

3. Contractor shall comply with all of its obligations set forth in Appendix B, "Supplemental Information for Contracts that Utilize Personally Identifiable Information."

4. Contractor has provided or shall provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its assignees, if any) who will have access to Protected Data, prior to their receiving access as follows:

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.

5. Contractor ☐ intends ☒ does not intend to utilize subcontractors, assignees or other authorized agents for the purpose of fulfilling one or more of its obligations under this Data Privacy Agreement. In the event that Contractor engages any subcontractors to perform its obligations under this Data Privacy Agreement, it shall ensure such subcontractors abide by the data protection and security requirements contained in this Data Privacy Agreement and applicable state and federal law by methods as more fully described in Appendix B, "Supplemental Information for Contracts that Utilize Personally Identifiable Information."
6. Contractor shall provide prompt notification to JCSD of any breaches or other unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Privacy Agreement. Contractor shall manage data security and privacy incidents that implicate Protected Data, including plans to identify breaches as follows:

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.

7. Contractor shall implement the procedures for the return, transition, deletion and/or destruction of Protected Data at such time that this Data Privacy Agreement expires or is terminated as more fully described in Appendix B, "Supplemental Information for Contracts that Utilize Personally Identifiable Information."