

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	Everyday Speech LLC <hr/>
PII Declaration	<p>Does your organization/software collect student personally identifiable information (PII) or staff PII?</p> <p>Examples of student PII:</p> <ul style="list-style-type: none"> 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; <p>Examples of staff APPR PII:</p> <ul style="list-style-type: none"> a. Teacher ID b. Name c. Birthdate d. Gender e. Race f. Salary <p><input type="checkbox"/> IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.</p> <p>If you collect the PII information above, please complete the remainder of this form.</p>
Description of the purpose(s) for which Contractor will receive/access PII	Using de-identified, aggregate, or anonymized user information for the purpose of research and development to improve the product offered by the Contractor.
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR PII

Contract Term	Contract Start Date <u>04/18/2023</u> Contract End Date <u>06/30/2024</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) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> • 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) <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:
Encryption	Data will be encrypted while in motion and at rest.



Western Suffolk BOCES - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

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.	On the network level we have Firewall, DDoS mitigation, Spoofing and Sniffing Protections, and Port Scanning blockers. All of the above are provided by our hosting service.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	While in transit, data is encrypted and transferred over HTTPS protocols using TLS encryption. Our hosting provider runs OS Vulnerability Scan and Security Event Monitoring. We don't have specific safeguard tasks performed in the application.
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 represents and warrants that any of its officers, employees, and/or assignees who will have access to student, teacher and/or principal data pursuant to the Original Agreement will receive training on the federal and state laws governing confidentiality of such student, teacher and/or principal data, prior to obtaining initial or any further access to such data. Federal and state laws include, but are not limited to, the Parents' Bill of Rights for Data Privacy and Security, Children's Online Privacy Protection Act, FERPA, and COPPA.
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.	All employees are bound by contract and kept up-to-date on our security and privacy practices. Only personnel who need off-line secure information to perform a specific job (for example, a Customer Service Specialist) are granted access to personally identifiable information.
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.	Our platform automatically restores customer applications and databases in the case of an outage. The platform is designed to dynamically deploy applications within the Heroku and AWS cloud, monitor for failures, and recover failed platform components including customer applications and databases. On the server side, our hosting provider has Fire Detection and Suppression, Power Redundancy, and Climate and Temperature Control. Preventative maintenance is performed to maintain the continued operability of equipment.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Yes, we have daily backups. Also if the user cancels we hold on to data in case they reactivate their account, but it can be permanently deleted at any time if a request is made.
7	Describe your secure destruction practices and how certification will be provided to the EA.	If the user cancels, we hold on to data in case they reactivate their account, but it can be permanently deleted at any time if a request is made. We manually run a "Delete" query on the related database records. The data is verified to have been deleted if our database returns no results.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	We are compliant with COPPA and FERPA. All data is stored in servers located in the continental USA. Compliance with ISO 27001, 27017, 27018 and SOC 1, 2, 3.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Available upon request



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]	<i>Cal Brunell</i>
[Printed Name]	Cal Brunell
[Title]	Co-Founder
Date:	04/18/2023

January 13, 2022



PDFfiller Document ID: 8D55-4B1E-B78F-0002