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 _____
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	Provision of the Platform. We may use personal information and usage information to support the delivery of our services on the Platform. Support the Platform. We may use the information provided us to service any customer support requests, including troubleshooting problems and monitoring such requests. Improve the Platform. We may use the information provided us to customize, measure, and improve the Platform through various analytical methods and user research. Protect the Platform. We may need to use the information to protect our rights, prevent fraud, and keep the security of Everyday Speech, our employees, our customers, and district data.
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR PII

PDFfiller Document ID: 0A9D-7EA7-75A1-0002

Contract Term	Contract Start Date 11/19/2026 Contract End Date 11/18/2027
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: 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.
Encryption	Data will be encrypted while in motion and at rest.

PDFfiller Document ID: 0A9D-7EA7-75A1-0002

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.	See Additional Information below
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See Additional Information below
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.	See Additional Information below
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.	See Additional Information below
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.	See Additional Information below
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	See Additional Information below
7	Describe your secure destruction practices and how certification will be provided to the EA.	See Additional Information below
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	See Additional Information below
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Please refer to NIST Cybersecurity Framework Table: https://drive.google.com/file/d/12_SSbotIZaCr32FB5N2IxH9WtdibEc9A/view?usp=sharing

Additional Information (More information can be provided at the bottom 2 pages):

PDFfiller Document ID: 0A9D-7EA7-75A1-0002

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]	Lily Rego Verified by pdfFiller 11/19/2026
[Printed Name]	Lily Rego
[Title]	Chief Operating Officer
Date:	11/19/2026

Version: 4/30/25

PDFfiller Document ID: 0A9D-7EA7-75A1-0002

Additional Information:

1. During the term of the Agreement, Contractor will implement all state, federal and local data security and privacy requirements, consistent with the School District's Data Security and Privacy Policy in the following way(s):
(1) To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework;
(2) Not to sell, use or disclose personally identifiable student, teacher or principal data or information for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;
(3) To limit internal access within the Service Provider to personally identifiable student, teacher and principal information and data of the School District to only those officers, directors, employees, or authorized sub-contractors or assignees of the Contractor that are determined to need access to such records or data to perform the services set forth in the Agreement.

2. Data Storage - All Protected Information is stored and processed electronically on Amazon Web Services, and our employees do not have physical access to the hardware where Protected Information is stored. - All AWS hosted infrastructure is monitored with anomalous activity alerting through our Cloud Observability platform which is combined with service and port restrictions on the individual AWS resources.

Background Checks - All new employees receive a standard background check upon accepting an offer of employment. Employees who access Student PII or would otherwise interact with a student or be on a school campus are required to pass an FBI fingerprinted background check.

Devices - All Employees are required by policy to use Company owned laptops. All company owned devices are enrolled in Device Management programs which apply a secure configuration baseline, including centralized control of hard drive encryption and key escrow. The administrative controls provided by the Device Management software prevents employees from removing or loosening centrally applied security configurations. All employees are required to complete training on the best practices for secure use of their company-owned devices, including practices to follow to limit the possibility of unauthorized disclosure.

Unauthorized Disclosures - All Employees are explicitly bound by an Acceptable Use Policy and Data Classification Policy. The practices in these policies are implemented across the company and include a data category for the treatment of the most sensitive data, such as Student PII. Furthermore, they outline instructions for what to do if this data is stored or accessible in an unauthorized place, and disciplinary measures for unauthorized access or distribution of Student PII or other Restricted information.

Access Controls - Contractor has administrative and technical controls requiring role-based access controls according to the principle of least privilege. User provisioning and password complexity adheres to commonly accepted practice with mandatory MFA for all sessions, privileged or otherwise, where technically feasible.

Encryption - All systems that transmit confidential information use TLS 1.2 or later with 128-bit or larger keys. Data at rest is encrypted within the database using Authenticated Encryption with Associated Data (AEAD) algorithms employing 256-bit encryption keys. Confidential information is not extracted, transformed or processed outside of the database. Access to encryption keys is controlled through role based access control.

Vulnerability Management - Contractor’s Vulnerability Management policy requires a third party risk assessment with penetration testing on at least an annual basis. Internal vulnerability management practices incorporate daily host based scans and weekly external scans. Critical or High findings are documented, prioritized and remediated within the documented timeframe commensurate with published policy.

Operational Monitoring - The Everyday Speech platform is integrated with real-time performance monitoring to identify unusual spikes in activity, anomalous traffic patterns, or to identify other unusual behavior.

Incident Response - Contractor’s incident response plan adheres to commonly accepted industry standards and is tested through table-top scenarios on a regular basis.

3. Contractor represents and warrants that any of its officers, employees, and/or assignees who will have access to protected student, teacher and/or principal data receive training on the federal and state laws governing confidentiality of such protected student, teacher and/or principal data, prior to obtaining initial or any further access to such data. These training sessions are done through an LMS platform and includes mandatory videos and quizzes on the materials. Remediatory training is required before accessing protected data if a passing score is not attained on the quiz. The training materials currently cover NYS Education Law 2-D, COPPA and FERPA and must be completed at least annually.

4. All employees are bound by contract and kept up-to-date on our security and privacy practices, and Protected Information access is generally limited to these employees. Subcontractors are utilized in developing and distributing the platform, but do not have responsibilities that involve access to Protected Information. The only subprocessor that processes or accesses Protected Information for the platform is AWS, where the agreement with them has security and privacy controls that are at least as stringent as those required by state and federal laws and the NYSED in this Agreement.

5. Contractor’s Incident Response Plan identifies standard definitions of a privacy or security related event and the communication mechanisms to report events. If a suspicious event is reported by an individual or security or monitoring system to the Security and Privacy Council, the event is assumed to be a security incident until proven otherwise.

Upon initial observation of unusual or unexpected activity, a suspected Security Incident must be declared if the initial observer believes the event is relevant to the confidentiality, availability, integrity, or privacy of Everyday Speech controlled data, systems or networks. After declaring the suspected Security Incident, the initial observer:
may delegate the initial observer responsibilities to someone on the security and privacy council if appropriate
must create a dedicated, private slack channel devoted to the incident
ensure the initial tracking Asana task is created
assume the role of Incident Manager
adhere to documented escalation and internal reporting guidelines
contact relevant team members necessary to properly analyze and investigate the activity and invite each to the incident Slack channel
relinquish the role of Incident Manager as appropriate

Upon confirmation of a security incident, the response plan outlines defined criteria to assist the response team in establishing an initial severity, which drives reporting and escalation requirements.

Critical Severity Incidents - Require an immediate notification to the Director of Information Security and Senior Director of Engineering and Product. While the incident is active, hourly notifications and updates must be provided to the Senior Director of Engineering and Product so they can facilitate communication to the Executive Leadership Team and the rest of the organization.

High Severity Incidents - Require an immediate notification to the Director of Information Security. While the incident is active, notifications and updates should be provided every two hours to the Senior Director of Engineering and Product so they can facilitate communication to the Executive Leadership Team and the rest of the organization.

Medium & Low Severity Incidents - Require an immediate notification to the Director of Information Security. While the incident is active, notifications and updates should be provided as necessary to the Senior Director of Engineering and Product so they can facilitate communication to the Executive Leadership Team and the rest of the organization

The incident response plan adheres to the recommendations outlined by NIST. All incidents must be documented with as much detail as technically possible for reference and internal tracking. At the conclusion of any reported incident, a written incident report must be completed and delivered to the Executive Leadership team. Additionally, in order to close out an incident, a retrospective or lessons learned session must be conducted. Any actionable recommendations or process improvements noted in the retrospective are documented and implemented as appropriate.

All communication from confirmation through investigation, remediation and recovery are confined to a limited, controlled communication channel. The breach notification to the district will be sent within 7 business days or sooner, if contractually required. Following any security incident, a ‘lessons learned’ session must be conducted to document gaps in the plan, recommendations for improvement, and root cause analysis.

Everyday Speech has a strict policy against the unauthorized disclosure of Protected Information. Furthermore, employees rarely access PII so most common situations for unauthorized disclosures would not be practical. However, if such a scenario were to happen, the Incident Response Plan would still be applicable for dealing with the situation in accordance with the requirements of the NYSED.

PDFfiller Document ID: 0A9D-7EA7-75A1-0002

Additional Information:

6. At termination or expiration of services, Everyday Speech will meet or exceed the NIST SP 800-88 guidelines in destroying all District Data on its platform by deleting all it from our databases with a DELETE query within 30 days, or sooner if requested or contractually required. The data will be deleted from back-ups in the following 7 days. At any point in time up until the data is destroyed, the district may request a copy of the data.

7. At termination or expiration of services, Everyday Speech will meet or exceed the NIST SP 800-88 guidelines in destroying all District Data on its platform by deleting all it from our databases with a DELETE query within 30 days, or sooner if requested or contractually required. The data will be deleted from back-ups in the following 7 days. When the Protected Data is destroyed, we will send an email to the EA certifying that the process was successful.

8. Everyday Speech agrees to abide by all relevant federal, state, and local data privacy and security regulations including the following:
Family Educational Rights and Privacy Act (FERPA): Student PII is never sold or used for marketing purposes and is only collected, stored or used for authorized purposes (legitimate educational interests).
Children's Online Privacy Protection Rule (COPPA): Similar to other students under FERPA, consent to use and process PII on the platform is granted through the educational institution, and the platform only uses the data within an educational context and not for marketing or similar commercial purposes. NYS Education Law 2-D: The platform has the least intrusive data collection policies practicable for the platform goals. Similarly, the data that is collected is accessible to the minimal amount of people to use and maintain the platform.
Children's Internet Protection Act (CIPA): All content on the platform that a student will see is either produced by Everyday Speech or manually added by the district's educators.
Individuals with Disabilities Education Act (IDEA): The Everyday Speech platform does not specifically collect IEP, disability or diagnosis data, but an educator may enter IEP data, such as when planning a session and adding session notes. This IEP data is intended only for informational purposes for the educator to use in future product sessions (and is deleted at the termination of services with other District Data.) The platform is designed to be part of an IEP's implementation and not the central place where a specific IEP is stored and tracked. The platform is built to limit the student data to the educator specific to that student.
Pupil Privacy Protection Amendment (PPRA): Everyday Speech does not conduct surveys, analyses, or evaluations of students for any of the eight protected areas of the PPRA

PDFfiller Document ID: 0A9D-7EA7-75A1-0002