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	Prentke Romich Company dba PRC-Saltillo _____
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	The exclusive purpose for which the Contractor is being provided access to ProtectedInformation is to provide the product or services that are the subject of this Contract to the EA.The product or services are used to provide augmentative and alternative communication and support for nonverbal students.
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR PII

PDFfiller Document ID: 8532-7E81-7345-0000

Contract Term	Contract Start Date 11/09/2026 Contract End Date 11/09/2027
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: PRC-Saltillo has strict access controls that follow a least privileged model. Datais encrypted at rest and in motion. Access to these systems is reviewed yearly.Patching occurs every 30 days or less and know vulnerabilities are mitigated orpatched as soon as patches are available.
Encryption	Data will be encrypted while in motion and at rest.

PDFfiller Document ID: 8532-7E81-7345-0000

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.	Data not used for commercial purposes. Any data uploaded has secure SSL encryption protected by 256-bit encryption at rest. 3rd party contractors have no access to data.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Encryption at motion/rest, least priv access, patch every 30 days, immediately if vulnerability (scans),network segmentation, no local admin rights, audit Logs, endpoint security.
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.	Employees are trained on data privacy upon hire and training is updated on a yearly basis.
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.	PRC-Saltillo will not utilize subcontractors. Employees are trained on privacy and security of client information and complete a confidentiality agreement.
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.	Use Threat Detection Services from Security Vendor to detect and alert for intrusions; Regularly patch web servers and stay informed on vulnerabilities; Run quarterly scans to find vulnerabilities in websites and implementing penetration testing.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	PRC-Saltillo will consult with the EA on the method in which they would prefer to receive the data.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Users control their data in iShare,deleted datanot backed up after 2-weeks is rendered unrecoverable by PRC-Saltillo. No user data collection unless enabled. In TouchChat, collected data stays on board the app.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Our data security and privacy practices alignwith Ed Law 2-d and Section 121 of theCommissioners Regulations.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	Our data security and privacy practices align with the NIST Cyber Security core framework to identify, protect, detect, respond, and recover.

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

PDFfiller Document ID: 8532-7E81-7345-0000

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]	Hedi Garber Signed • Nov 9, 2026
[Printed Name]	Hedi Garber
[Title]	Strategic Partnerships/Accounts Specialist
Date:	11/09/2026

Version: 4/30/25

PDFfiller Document ID: 8532-7E81-7345-0000

Additional Information:

PDFfiller Document ID: 8532-7E81-7345-0000

Additional Information:

PDFfiller Document ID: 8532-7E81-7345-0000