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	eMATHinstruction, Inc. _____
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	We collect teacher name and email address only for the purposes of providing access to mathematics materials.
Type of PII that Contractor will receive/access	Check all that apply: ☐ Student PII ☐ APPR PII

PDFfiller Document ID: D385-7E7E-9E83-0000

Contract Term	Contract Start Date 07/01/2026 Contract End Date 06/30/2027
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: See attached data security compliance document.
Encryption	Data will be encrypted while in motion and at rest.

PDFfiller Document ID: D385-7E7E-9E83-0000

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.	See below data security compliance information.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See below data security compliance information.
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.	We provide yearly training for all employees through Traliant.
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 below data security compliance 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.	See below data security compliance information.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	See below data security compliance information.
7	Describe your secure destruction practices and how certification will be provided to the EA.	See below data security compliance information.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	See below data security compliance information.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	See below data security compliance information.

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

PDFfiller Document ID: D385-7E7E-9E83-0000

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]	Darlene Pastore Signed • Nov 8, 2026
[Printed Name]	Darlene Pastore
[Title]	Director of Operations
Date:	11/08/2026

Version: 4/30/25

PDFfiller Document ID: D385-7E7E-9E83-0000

Additional Information:

EMATHINSTRUCTION DATA SECURITY AND PRIVACY COMPLIANCE MEASURES For School Districts Requesting Information on Data Security and Privacy Compliance with 2-d and Section 121.3 (Version April 2020) What data do we receive from schools and why? □ We DO NOT ask for, collect, or receive any student data. □ We DO NOT ask for, collect, or receive any principal data. □ We DO NOT ask for, collect, or receive any educational data including grades, test scores, disciplinary information, or educational information. □ We ask for, collect, and receive teacher name and email address ONLY. This is information is used for the purpose of maintaining user accounts. These user accounts provide user access to mathematics materials for educational purposes only. How do we implement State and Federal data security and privacy requirements throughout the life of the contract? □ We make reasonable efforts to comply with NIST Cybersecurity Framework guidelines. □ We use data encryption technology to secure the transfer of user data and we comply with PCI compliance requirements. We also limit access to any and all user data to only our team members to help fulfill orders, process refunds, and support you. We will not sell or share your personal data with any third parties without your prior consent except where we are required to do so by law. □ We limit access to PII so that no personnel (whether employee or independent contractor or vendor) has access to PII unless their essential job/contract function requires such access; and in such cases we limit their access to only that PII required for them to perform their essential job/contract function. □ We do not collect student data, teacher data or principal data from school districts. □ Our Privacy Policy, which is published and made prominent on our website, clearly communicates what data we collect, how that data is used, how a user may obtain a copy of the data collected about them, and how a user may challenge the accuracy of the data collected or received about them. How do we implement data security and privacy requirements that are compliant with the district's data security and privacy policy throughout the life of the contract? □ We use industry-recognized security safeguards to protect the personally identifiable information that you have provided to us from loss, misuse, or unauthorized alteration. □ We securely transfer all data over encrypted connections and store all user data on our web servers only, for our users' privacy. The only data shared with third- party services is general, anonymized data containing no personal identifying information. No personal data is sold or shared with any third parties without your prior consent except where we are required to do so by law. □ We have a Personal Data Exporter and Removal policy in place and up to date to export/remove personal data associated with all users accounts to meet privacy compliance laws. We comply with Section 121.3(c) of the Commissioner's Regulations by: 1. Not receiving from the school district any student data, teacher data or principal data; 2. Limiting access to PII in compliance with the parent's bill of rights for data privacy and security, as set forth in greater detail in other sections of this document; 3. Using data security technology and methods, such as encryption, HTTPS and regular plugin security updates, to ensure such data will be protected and data security and privacy risks mitigated, while in motion or at rest, as set forth in greater detail in other sections of this document; 4. Abiding by eMATH's Internal Data Security and Privacy Compliance Policy, which is informed by NIST Cybersecurity Framework guidelines for small business. 5. Publishing in eMATH's Privacy Policy how a parent, student, eligible student, teacher or principal may challenge the accuracy of any teacher or principal data collected. How will our employees and any assignees with access to student data, teacher data or principal data receive training on the relevant confidentiality laws before receiving access to such data? □ We will ensure that no employee or assignee will receive access to PII unless such access is necessary for them to perform their job functions. AND □ We will ensure that before any employees or assignees are granted access to PII or to any part of the system from which PII may be accessed, the employee or assignee must first read and agree to abide by eMATH's Internal Data Security and Privacy Policy. eMATH from time to may from time to time use subcontractors, who may or may not have access to PII. □ We will ensure that no subcontractor will receive access to PII unless such access is necessary for them to perform the contracted-for services AND □ We will ensure that before any subcontractors are granted access to PII or to any part of the system from which PII may be accessed, the subcontractor must first read and agree to abide by eMATH's Internal Data Security and Privacy Policy. Our action plan for handling any breach or unauthorized disclosure of PII is: Upon learning of a data breach or unauthorized disclosure, we will promptly: 1. Notify our IT services provider and instruct them to immediately implement technical measures to limit the extent of the breach and secure all uncompromised data; 2. Notify all contracted school districts of the breach or unauthorized disclosure; 3. Notify the owners of the PII (which includes the parents of any minor students) of the breach or unauthorized disclosure; 4. Notify our attorney;5. Begin an investigation to identify the source of the breach, in particular, whether it originated internally, and to remove system access from any employees, assignees or subcontractors suspected of causing or contributing to the breach or unauthorized disclosure. 6. Implement the continuation plan using backup systems and equipment as necessary while the main system is undergoing forensic investigation and cleaning. 7. Notify any insurers providing cybersecurity coverage to eMATHinstruction and/or any contracted school districts. When the school district contract ends or is terminated, eMATH will, within 30 days after the effective termination date: 1. Permanently delete from all local equipment and all servers, all data received from the school district over the course of the contract unless the school district, during that 30day period, delivers written instructions to eMATHinstruction to return the data to the school district, except that eMATH may retain teacher name and teacher email address for the purpose of facilitating future orders from the school district or teacher. 2. If eMATH, during that 30-day period, receives from the school district written instructions to return the data to school district, eMATH will do so by transmitting to the school district, in electronic form in one or more encrypted files, all data received from that school district over the course of the contract. After such transmission, eMATH will review its system to ensure any copies of that school district's data have been permanently delete

PDFfiller Document ID: D385-7E7E-9E83-0000

Additional Information:

PDFfiller Document ID: D385-7E7E-9E83-0000