Williamson Central School

Williamsoncentral.org
(315) 589-9661

PO Box 900
Williamson, NY, 14589

E. Bridget Ashton
Superintendent of Schools

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Williamson Central School District ("Williamson CSD") and Heinemann, a division of Greenwood Publishing Group LLC ("Vendor") are parties to the privacy policy at https://www.heinemann.com/products-privacy-policy/?utm_medium=shorturl&utm_source=products-privacy ("the underlying contract" or "Service Agreement") governing the terms under which Williamson CSD accessed, and Vendor provides, Math Expressions and Matific ("Product(s)" or "Service(s)"). Williamson CSD use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1 "Breach"means 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 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.

2.2 "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.

2.3 "Disclose"means 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.

2.4 "Education Record" means, 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.

2.5 "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from Williamson CSD or is created by the Vendor's product or service in the course of being used by Williamson CSD.

2.6 "Vendor/Contractor" means Heinemann, a division of Greenwood Publishing Group LLC - who provides a digital platform for students to practice a variety of math skills.

2.7 “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; and for purposes of this Contract specifically includes Williamson CSD.

2.8 “Williamson CSD” means the Williamson Central School District.

2.9 “Parent” means a parent, legal guardian, or person in parental relation to a Student.

2.10 “Student” means any person attending or seeking to enroll in an educational agency.

2.11 “Eligible Student” means a student eighteen years or older.

2.12 “Assignee” and “Subcontractor” shall each mean any person or entity, including third party service providers, that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.13 “This Contract” means the underlying contract as modified by this Addendum.

2.14 “Encrypt or Encryption” 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.

2.15 “NIST Cybersecurity Framework”: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

2.16 “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.

2.17 “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. The School is part of the Williamson Central School District.

2.18 “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.

2.20 “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.

3. Compliance with Law

In order for Contractor to provide certain services ("Services") to the EA pursuant to the underlying contract; 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.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance

with the Williamson CSD POLICY 8154 - Privacy and Security for Student Data and Teacher and Principal Data, a copy of which is Attachment B to this Addendum. If there is any conflict between this Contract Addendum and any attachment, this Contract Addendum will control and take precedence.

5. 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. The Contractor may use de-identified information, as is defined by FERPA, for evaluation, research and development of educational products and services.

6. 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 the EA's policies, attached to this DPA. Education Law Section 2-d requires that Contractor provide the EA 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 Attachment D.

7. Right of Review and Audit.

Upon written request by the EA, the Contractor shall provide the EA with copies of its policies and summaries of 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, the EA's policies applicable to Contractor attached to this DPA, and alignment with the NIST Cybersecurity Framework. Such audits shall be made no more than once per year, during normal business hours, and not take than one (1) business day. Such audits shall be subject to the execution of Contractor's confidentiality agreement containing reasonably standard terms, and scheduling according to the mutual convenience of the parties.

8. Vendor Employee Training

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

9. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from Williamson CSD or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students. The Vendor may use de-identified information for evaluation, research and development of educational products and services.

10. Ownership and Location of Protected Information

10.1. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with Williamson CSD. Vendor shall acquire no ownership interest in education records or Protected Information.

10.2. Williamson CSD shall have access to the Williamson CSD's Protected Information at all times through the term of this Contract. Williamson CSD shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

10.3. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by Williamson CSD or its authorized users, or performing any other data analytics other than those required to provide the Product to Williamson CSD. Vendor is allowed to perform industry standard back-ups of Protected Information.

10.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada.

11. Purpose for Sharing Protected Information

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to Williamson CSD.

12. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same or equally restrictive obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

13. Data Subject Request to Amend Protected Information

13.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the Williamson CSD for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

13.2. Vendor will reasonably cooperate with Williamson CSD in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

14. Vendor Data Security and Privacy Plan

14.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment D to this Contract and made a part of this Contract.

14.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

14.3. align with the NIST Cybersecurity Framework 1.1;

14.4. equal industry standards including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

14.5. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the Williamson CSD data security and privacy policy (Attachment B);

14.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

14.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

14.8. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

14.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

14.10. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify Williamson CSD; and

14.11. describe whether, how and when data will be returned to Williamson CSD, transitioned to a successor contractor, at Williamson CSD's option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

15. Contractor's Employees and Subcontractors.

15.1. 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 require that all such employees and subcontractors comply with the terms of this DPA or equally restrictive data security obligations.

15.2. Contractor must require 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.

15.3. 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: 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 industry standards. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

15.4. Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.

15.5. Contractor must not disclose PII to any other party except to third party service providers and subcontractors necessary to provide the service and unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

16. Additional Vendor Responsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

16.1.0. Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors or third party service providers that need access to provide the contracted services;

16.1.1. Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

16.1.2. Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the Williamson CSD unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to Williamson CSD no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

16.1.3. Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

16.1.4. Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

16.1.5. Vendor will notify the Williamson CSD of any confirmed data breach resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the confirmation of the breach; and

16.1.6. Where a breach or unauthorized disclosure of Protected Information is solely attributed to the Vendor's negligence or omission, the Vendor shall pay for or promptly reimburse Williamson CSD for the full actual cost incurred by Williamson CSD to send notifications required by Education Law Section 2-d.

17. Termination

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

18. Data Return and Destruction of Data.

18.1. Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copyof 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 the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, with sixty (60) day written notice, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.

18.2. If applicable, once the transfer of PII has been accomplished in accordance with the EA's sixty (60) day 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.

18.3. Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

18.4. 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 without also requiring the third party not to reidentify.

19. Commercial or Marketing Use Prohibition.

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

20. 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.

21. Breach.

21.1. Contractor shall promptly notify the EA of any confirmed Breach of PII without unreasonable delay no later than seven (7) business days after confirmation 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 the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA may 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.

21.2. Notifications required under this paragraph must be provided to the EA at the following address:

[Name: Mikala Smolinski

Title: Data Protection Officer

Address: PO Box 900

City, State, Zip: Williamson, NY, 14589

Email:] msmolinski@williamsoncentral.org

22. Cooperation with Investigations.

Contractor agrees that it will reasonably cooperate with the EA 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 solely attributable to Contractor or its Subcontractors's negligence or omission.

23. Notification to Individuals.

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

24. 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.

25. PARENT AND ELIGIBLE STUDENT PROVISIONS 25.1. 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 the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA 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 the EA and refer the Parent or Eligible Student to the EA.

25.2. 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 Attachment A and Attachment C, respectively, and incorporated into this DPA. Contractor shall complete and sign Attachment C and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Attachment C on its website.

26. MISCELLANEOUS

26.1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Attachments 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.

26.2. 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.

Signatures

For Williamson CSD	For Heinemann , a division of Greenwood Publishing Group LLC
Mikala Smolinski	Ashley Poreda
Date	**Date**
4/16/25	Ashley Poreda, Lead Contracts Specialist, 4/16/2025

Williamson Central School

Williamsoncentral.org
(315) 589-9661

PO Box 900
Williamson, NY, 14589

E. Bridget Ashton
Superintendent of Schools

Attachment A - Parents' Bill of Rights for Data Privacy and Security

The Williamson Central School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of 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 the EA at: https://forms.gle/yM7qdAibzvDJdM4KA or completing the form and mailing the form to the district's Data Protection Officer at the following address: Data Protection Officer
   PO Box 900
   Williamson, NY, 14589
7. Complaints may also be submitted to the NYS Education Department at https://www.nysed.gov/data-privacy-security/parents-and-students-file-privacy-complaint, 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.
8. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
9. 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.
10. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Mikala Smolinski 4/16/25

Williamson Central School Date

Ashley Poreda 4/16/2025

Heinemann, a division of Greenwood Publishing Group LLC Date

Ashley Poreda, Lead Contracts Specialist 4/16/25

Attachment B - Privacy and Security for Student Data and Teacher and Principal Data

https://resources.finalsite.net/images/v1690821847/williamsoncentralorg/p44xlhqigoskgd4itzdz/PrivacyandSecurityforStudentDataandTeacherandPrincipalData.pdf

Attachment C- 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	**Heinemann, a division of Greenwood Publishing Group LLC**
Description of the purpose(s) for which Contractor will receive/access PII	**Heinemann will only use data in connection with District's use of HMH's products.**
Type of PII that Contractor will receive/access	**Check all that apply:** X **Student PII** ☐ **APPR Data**
Contract Term	**Contract Start Date 4/8/2025** **Contract End Date 4/7/2026**
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.** X **Contractor will utilize subcontractors.**

Data Transition and Secure Destruction	**Upon expiration or termination of the Contract, with sixty (60) days written notice, 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 30 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)** **X 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:** HNM stores all data in an AWS Hosting facility in the United States. HMH has implemented and maintains reasonable organizational, technical, and administrative controls and is responsible for the development, opera on, maintenance, and use of our cloud-hosted applications and data required for customers to participate in our learning platforms. Physical security controls are managed by our hos ng partner, Amazon Web Services (AWS). Our data management procedures include the following: all user data are encrypted using standard Internet protocols; all user data on our interface are transferred over HTTPS; all user data in transit are protected by TLS 1.2; all user data are housed on a scalable hosting architecture; all user data are stored behind AES-256 encryption algorithms. For additional information, please refer to HNM's Privacy Policy at https://www.heinemann.com/products-privacy-policy/?utm_medium=shorturl&utm_source=products-privacy

Encryption	**Data will be encrypted while in motion and at rest.**

CONTRACTOR	
[Signature]	Ashley Poreda
[Printed Name]	**Ashley Poreda**
[Title]	**Lead Contracts Specialist**
Date:	**4/16/25**

Attachment D – Vendor's Data Security and Privacy 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.	All HNM data privacy and security practices are implemented to comply with all applicable law and in accordance with the Privacy Policy: https://www.heinemann.com/products-privacy-policy/?utm_medium=shorturl&utm_source=products-privacy and Terms of Purchase: https://www.heinemann.com/terms-of-purchase/
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	HNM has implemented and maintains technical, administrative, and physical security controls that are designed to protect the security, confidentiality, and integrity of personal information collected through our learning platforms from unauthorized access, disclosure, use, or modification. Our data management procedures include the following: all user data are encrypted using standard Internet protocols; all user data on our interface are transferred over HTTPS; all user data in transit are protected by TLS 1.2; all user data are housed on a scalable hosting architecture; all user data are stored behind AES-256 encryption

		algorithms. For additional information, please refer to https://www.heinemann.com/products-privacy-policy/?utm_medium=shorturl&utm_source=products-privacy and Terms of Purchase: https://www.heinemann.com/terms-of-purchase/
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 conducts periodic security awareness training intended to enhance employees understanding of sound security practices and covers a wide variety of topics relative to security, including annual Security Awareness Training that addresses Data Privacy. The contractor also has Personally Identifiable Informa on (PII) and Data Classification Policies that employees are required to acknowledge, as well as a very aggressive 'appropriateness of access' policy where employees who have access to any system/data have their access level reviewed quarterly. All training is conducted by the Information Security department.
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.	HNM requires for all employees and subcontractors to abide by all HNM data privacy and security practices are implemented to comply with all applicable law and in accordance with the https://www.heinemann.com/products-privacy-policy/?utm_medium=shorturl&utm_source=products-privacy and Terms of Purchase: https://www.heinemann.com/terms-of-purchase/
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.	Contractor has implemented and maintains technical, administrative, and physical security controls that are designed to protect the security, confidentiality, and integrity of personal information collected through our learning platforms from unauthorized access, disclosure, use or modification. Contractor's information security controls comply with reasonable and accepted industry practice, as well as requirements under COPPA and FERPA. Contractor diligently follow these information security controls and periodically review and test our information security controls to keep them current.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon 60 day written notice, data will be returned in a mutually agreed upon format or disposed using industry standards.
7	Describe your secure destruction practices and how certification will be provided to the EA.	We use industry standard disposal practices and will provide EA with certification that data has been disposed upon written request.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	All HNM data privacy and security practices are implemented to comply with all applicable law and in accordance with the Privacy Policy: https://www.heinemann.com/products-privacy-policy/?utm_medium=shorturl&utm_source=products-

		privacy and Terms of Purchase: https://www.heinemann.com/terms-of-purchase/
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

Attachment D.1 – NIST CSF TABLE

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Yes
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**Yes. Regular company, division and departmental meetings.**
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**We have a matrix of IT and business Controls that are reviewed and tested throughout the year.**
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**Yes**
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**Yes**

	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**Yes**
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**Yes. IT Controls and documentation that is regularly reviewed and updated.**
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**Yes. We conduct security awareness training for all new employees. We conduct annual security awareness training for all employees. We conduct phishing testing and training throughout the year.**

	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**Yes**
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**Yes**
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**Yes**
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**Yes**
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**Yes**

	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**Yes**
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**Yes**
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**Yes**
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**Yes**
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**Yes**
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	**Yes**
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**Yes**
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**Yes**
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**Yes**
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**Yes**