

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).

<p>Name of Contractor</p>	<p>Houghton Mifflin Harcourt Publishing Company</p>
<p>PII Declaration</p>	<p>Does your organization/software collect student personally identifiable information (PII) or staff PII?</p> <p>Examples of student PII:</p> <ul style="list-style-type: none"> a. The student’s name; b. The name of the student’s parent or other family members; c. The address of the student or student’s family; d. A personal identifier, such as the student’s social security number, student number, or biometric record; e. Other indirect identifiers, such as the student’s date of birth, place of birth, and Mother’s Maiden Name; <p>Examples of staff APPR PII:</p> <ul style="list-style-type: none"> a. Teacher Id, 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 <p><input type="checkbox"/> IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.</p>
<p>Description of the purpose(s) for which Contractor will receive/access PII</p>	<p>HMH will use the data only in accordance with District's use of HMH products.</p>
<p>Type of PII that Contractor will receive/access</p>	<p>Check all that apply:</p> <p><input checked="" type="checkbox"/> Student PII</p> <p><input type="checkbox"/> APPR PII</p>

Contract Term	Contract Start Date <u>09/24/2024</u> Contract End Date <u>09/23/2025</u>	
Subcontractor Written Agreement Requirement	<p>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)</p> <p><input type="radio"/> Contractor will not utilize subcontractors.</p> <p><input checked="" type="radio"/> Contractor will utilize subcontractors.</p>	
Data Transition and Secure Destruction	<p>Upon expiration or termination of the Contract, Contractor shall:</p> <ul style="list-style-type: none"> • Securely transfer data to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data. 	
Challenges to Data Accuracy	<p>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.</p>	
Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>HMH 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, operation, 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 hosting 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 HMH’s K–12 Learning Platforms Privacy Policy at https://www.hmhco.com/privacy-policy-k12-learning-platforms. Additionally, access to data is based on a least-privileged model, where individuals are only granted the rights necessary to complete their job functions.</p>	
Encryption	Data will be encrypted while in motion and at rest.	

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

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN


The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	All HMH data privacy and security practices are implemented to comply with all applicable law and in accordance with the HMH K-12 Learning Platforms Privacy Policy (https://www.hmhco.com/privacy-policy-k12-learning-platforms) and Terms of Use (https://www.hmhco.com/web-terms-of-use)
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	All HMH data privacy and security practices are implemented to comply with all applicable law and in accordance with the HMH K-12 Learning Platforms Privacy Policy (https://www.hmhco.com/privacy-policy-k12-learning-platforms) and Terms of Use (https://www.hmhco.com/web-terms-of-use)
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 Information (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.	In the event that HMH subcontracts with an outside entity or individual in order to fulfill its obligations to the District, HMH ensures that it will only share the Data with such subcontractors if those subcontractors are contractually bound to observe the same obligations to maintain data privacy and security as required by HMH pursuant to the Agreement. HMH will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of the Data in its custody.
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 sixty (60) days written notice from the EA, Data will either be destroyed using industry standards or returned in a mutually agreeable format.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Upon sixty (60) days written notice from the EA, Data will either be destroyed using industry standards or returned in a mutually agreeable format.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	All HMH data privacy and security practices are implemented to comply with all applicable law and in accordance with the HMH K-12 Learning Platforms Privacy Policy (https://www.hmhco.com/privacy-policy-k12-learning-platforms) and Terms of Use (https://www.hmhco.com/web-terms-of-use)
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	All HMH data privacy and security practices are implemented to comply with all applicable law and in accordance with the HMH K-12 Learning Platforms Privacy Policy (https://www.hmhco.com/privacy-policy-k12-learning-platforms) and Terms of Use (https://www.hmhco.com/web-terms-of-use)

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]	
[Printed Name]	Catherine Crowe-Lile
[Title]	VP RFP, Bids & Contracts, and Sales Readiness Revenue Operations
Date:	September 24, 2024

March 12, 2024