

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” or “EA”) an Educational Agency, and Scholastic Inc. , inclusive of its affiliates (“Vendor” or “Scholastic” or “Contractor”) are parties to the Vendor’s end user license agreement (“the underlying contract” or “EULA”) governing the terms under which Williamson CSD accessed, and Vendor provides all digital education technology products listed at: <https://educationsolutions.scholastic.com/privacypolicy.html> and Mary Glasgow Learning Magazines (“MGM”).

(“MGM”) (“Product”). 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 in a manner which compromises its security or privacy, 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 Scholastic - who provides a digital subscription of content on current health and life skills resources.
- 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" shall mean an entity to which Vendor transfers its contractual rights hereunder including without limitation in the context of a merger or restructuring of Vendor. "and "Subcontractor" (as defined here) shall mean any person or entity 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" As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means 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.
- 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.
- 2.19
 "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. The EA acknowledges that Contractor will not collect any Teacher or Principal APPR Data in connection with the products to which this Agreement applies.

3. Compliance with Law

In order for Contractor to provide certain services ("Services") to the EA pursuant to Scholastic's end user license agreement ("Service Agreement" or "EULA"); 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.

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.

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. 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 summaries of its policies and 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, upon reasonable notice and written request from the EA, Contractor may be required no more frequently than once per 12-month period by the EA 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, and alignment with the NIST Cybersecurity Framework performed by an independent third party engaged by the Contractor at Contractor's expense, and provide the summary of the audit report to the EA. Contractor may provide the EA with a summary of a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit. Except as otherwise required by law or agreed in writing between the parties, and excluding Student Data or any other data that belongs to the EA, all information provided by Contractor to the EA pursuant to this paragraph or any audit or investigation shall be treated as Contractor's confidential information. The EA agrees that it will disclose such information only to such parties that the EA determines are necessary to assist it in its review and require such parties to enter into non-disclosure agreements or otherwise agree in writing to maintain its confidentiality. To the extent permitted by law, the EA will withhold such information from public disclosure.

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.

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 or otherwise inherent in the services or as described in the applicable privacy policy for data that is not PII. Vendor is allowed to perform industry standard back-ups of Protected Information. Reasonable documentation of back-up must be provided to Williamson CSD upon request.

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, Vendor will only share Protected Information with such entities if those entities are subject to the comparable obligations to maintain the privacy and security of Protected Information in accordance with New York Education Law Section 2-d and 8 NYCRR Part 121 as are required of Vendor under this Contract and all applicable New York State and federal laws. Scholastic ensures that its subcontractors and personnel engaged on an independent contractor basis will abide by such obligations through a combination of technical due diligence, trainings, contractual obligations, instructions, oversight, audits, and periodic tests, scans and other assessments, as appropriate.

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 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 best practices 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 ensure that all such employees and subcontractors comply with the terms of this DPA.
- 15.2. Contractor must ensure 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 take such actions required by applicable law or regulation or as Contractor deems appropriate in its good faith business judgment, which may include: notifying the EA and removing such subcontractor's access to PII; and, as applicable, retrieving all PII received or stored by such subcontractor and/or ensuring that PII has been securely deleted and destroyed in accordance with this DPA. 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 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:

- 16.1.1. Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;
- 16.1.2. Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;
- 16.1.3. 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;

- 16.1.4. Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;
- 16.1.5. 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);
- 16.1.6. Vendor will notify the Williamson CSD of any breach of security 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 discovery of the breach; and Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse Williamson CSD for the full cost incurred by Williamson CSD to send notifications required by Education Law Section 2-d. Except as otherwise required by law or agreed in writing between the parties, and excluding Student Data or any other data that belongs to the Educational Agency, all information provided by Vendor to the Educational Agency pursuant to this paragraph or any audit or investigation shall be treated as Vendor's confidential information. The Educational Agency agrees that it will disclose such information only to such parties that the Educational Agency determines are necessary to assist it in its review and require such parties to enter into non-disclosure agreements or otherwise agree in writing to maintain its confidentiality. To the extent permitted by law, the Educational Agency will withhold such information from public disclosure.

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 pursuant to the Service Agreement.

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 copy, summary or extract of 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 requested in writing by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, and upon written request from the EA, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.
- 18.3. 18.2 If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, upon written request from the EA, Contractor agrees to return, destroy, or de-identify 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, 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, upon written request from the EA, Contractor shall ensure that PII is securely deleted, de-identified, 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. Contractor shall be entitled to

retain archive copies required to be retained by law or to or to establish or defend against legal claims and back-up or log files not accessible in the ordinary course that are deleted on a standard schedule (other than ad hoc back-ups that are deleted outside standard retention windows). Upon written request, 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 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 unless such data is incapable of re-identification. If Contractor assigns its rights hereunder in connection with a merger, reorganization or sale of its business, it shall require the assignee to agree with the foregoing.

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 Breach of PII without unreasonable delay no later than seven (7) business days after discovery 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 shall 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 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 attributable to Contractor or its Subcontractors.

23. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, 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

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, to the extent of the conflict, 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

Mikala Smolinski

For Williamson CSD



For Scholastic Inc.

10/8/24

11/07/24

Date

Date

Williamson Central School

Williamsoncentral.org
(315) 589-9661

PO Box 900
Williamson, NY
14589

Marygrace Mazzullo
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 10/8/24

Williamson Central School Date

MLW

11/07/24

Scholastic Inc

Date

Attachment B - Privacy and Security for Student Data and Teacher and Principal Data
Attached hereto.


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	Scholastic Inc.
Description of the purpose(s) for which Contractor will receive/access PII	Contractor will receive PII data in order to provide all digital education products and MGM. See Contractor’s current list of digital education products at: https://educationsolutions.scholastic.com/privacypolicy.html The privacy policy for MGM can be found at: https://maryglasgowplus.com/privacy
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date <u>Commences as set forth in the applicable ordering document</u> Contract End Date <u>When subscription ends as set forth in the applicable ordering document, or is terminated.</u>
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors¹ 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) <input checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.

¹ Scholastic may engage some staff on an independent contractor basis, and Scholastic may use third party service providers on an enterprise basis, but Scholastic does not subcontract out any of the services subject to the agreement. Scholastic will require all third parties to comply with New York Education Law and 8 NYCRR Part 121.

Data Transition and Secure Destruction	<p>Upon expiration or termination of the Contract, and upon written request 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, de-identify, and/or 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 30 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. . (Amazon Web Services)</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>The security protection taken to ensure data will be protected include standards that will align with the NIST cybersecurity framework. Protected data is encrypted in motion (currently with TLS 1.2 128-bit encryption) and at rest (currently with 256 bit AES encryption). Contractor conducts periodic risk assessments and keeps audit trails and security logs to assess and remediate vulnerabilities and to protect data from deterioration or degradation. Additional measures include firewalls, anti-virus and intrusion detection, configuration control and automated backups. Data is classified by sensitivity, and access to data is rule- and role-based.</p>
Encryption	<p>Data will be encrypted while in motion and at rest.</p>

CONTRACTOR Scholastic Inc.	
[Signature]	
[Printed Name]	Matt Wilcox
[Title]	VP Digital Product Development
Date:	11/07/24

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.	See Exhibit D.1 Data Security and Privacy Plan.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See Exhibit D.1 Data Security and Privacy Plan.
3	Address the training received by your employees or other individuals or to the extent required by applicable law or regulation parties engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	See Exhibit D.1 Data Security and Privacy Plan.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound in accordance with legal and regulatory requirements to the requirements of the Contract, at a minimum.	See Exhibit D.1 Data Security and Privacy Plan.
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 Exhibit D.1 Data Security and Privacy Plan.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	See Exhibit D.1 Data Security and Privacy Plan.
7	Describe your secure destruction practices and how certification will be provided to the EA.	See Exhibit D.1 Data Security and Privacy Plan.
8	Outline how your data security and privacy program/practices align with the EA’s applicable policies.	Scholastic’s Data Security and Privacy plan covers the elements set forth in the agreement and applicable law, which means our program and practices align.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	<i>See Exhibit D.2 below</i>

Exhibit D.1 SCHOLASTIC INC. DATA SECURITY AND PRIVACY PLAN

In connection with the Contract Addendum (the “Addendum”) between Scholastic Inc. (“Vendor” or “Scholastic”) and the Williamson Central School District (the “District”), as amended, for the license of certain Scholastic products, Vendor acknowledges that it has read and can comply with the District’s Parents’ Bill of Rights for Data Privacy and Security, the provisions of which are hereby incorporated into this Data Security and Privacy Plan to the extent applicable to Vendor’s use and possession of student data subject to New York Education Law Section 2-d (“Protected Data”). Any capitalized terms not defined herein shall have the meanings given to them in the Addendum.

More specifically, and in furtherance thereof:

1. To implement all applicable data security and privacy requirements (whether by law, contract or policy of the applicable school, district, or other educational agency), Scholastic ensures that relevant staff are advised of data security and confidentiality requirements in district agreements and receive appropriate training (as described further below).
2. Scholastic only uses Protected Data as necessary to provide the licensed educational products and services for the benefit of the District, and access to Protected Data is limited to those employees or sub-contractors who need access for Scholastic to provide such products or services. On expiration of the applicable license agreement and at the District’s written request, Protected Data will be destroyed, returned or de-identified as set forth in the Addendum. The term of the license agreement is as indicated in the agreement, order form or similar document entered into by the parties.
3. Scholastic may retain subcontractors or service providers to assist it in performing services for and providing products to educational agencies. Scholastic does not share Protected Data with third parties other than subcontractors or service providers who are subject to contractual confidentiality and data security obligations, and who may not use the protected data for their own purposes. Scholastic ensures that its personnel, subcontractors and service providers will abide by such obligations through a combination of technical due diligence, trainings, contractual obligations, instructions, oversight, audits, and periodic tests, scans and other assessments.
4. If a parent or eligible student requests to see or challenge the accuracy of any student data, Scholastic’s standard procedure is to refer any such inquires to the participating educational agency and await further instruction. Scholastic will comply with the applicable participating educational agency’s procedure for access to or amendment of education records, subject to applicable law.
5. Scholastic retains data collected through the products for as long as reasonably necessary to provide the product or services and as specified in the applicable contract or otherwise directed by the educational customer.
6. To protect the security, confidentiality and integrity of protected New York state education data, Scholastic will utilize reasonable administrative, technical, operational and physical safeguards and practices including without limitation the following:
 - a. Scholastic stores and processes student data in accordance with industry standards including implementing appropriate administrative, physical and technical safeguards to protect it against unauthorized access, disclosure, alteration and use. Such safeguards align with the NIST Cybersecurity Framework.

- b. Scholastic personnel are required to sign a company confidentiality policy upon hiring, which covers customer information.
 - c. Physical security measures include security personnel and ID-only building access.
 - d. Data is classified by sensitivity, and access to data is rule- and role-based. Internal Vendor personnel access to Protected Data is further protected by multi-factor authentication and VPN requirements.
 - e. With respect to electronic data, no data is stored in “terrestrial” servers.
 - f. Scholastic conducts periodic risk assessments and keeps audit trails and security logs to assess and remediate vulnerabilities and to protect data from deterioration and degradation. Additional measures include firewalls, anti-virus and intrusion detection, configuration control and automated backups. Sensitive data is encrypted in transit (as of the date of the Addendum, with TLS1.2 128-bit encryption) and at rest (as of the date of the Addendum, with 256-bit AES encryption).
 - g. With respect to school users, Scholastic limits unsuccessful logon attempts, enforces minimum password complexity (unless the participating educational agency opts to utilize an “easy log-in” option available in some products for students in K-2 who may have difficulty with traditional log-in, for example pre-literate students, if available in a given product), and employs cryptographic mechanisms to protect the confidentiality of remote access sessions.
7. Without limitation of other training programs that Scholastic may utilize from time to time, Scholastic has provided and will provide the following data security and privacy awareness training to officers and staff with access to Protected Data:
- a. In-person group training sessions on children’s privacy and student privacy, covering applicable laws and best practices.
 - b. Third party online / interactive training sessions on privacy matters and data security available within company intranet and learning resources library.
 - c. Customized/proprietary Scholastic online / interactive training on the Children’s Online Privacy Protection Act available within company intranet and learning resources library.
 - d. In-house written guidelines on children’s privacy compliance available through company intranet.
 - e. Ongoing advice and counsel from in-house and external legal and technical advisors.
8. If Scholastic becomes aware of a security breach that results in the unauthorized release of Protected Data in its possession or control (whether directly or via a subcontractor or third party service provider) in violation of applicable law or contractual obligation, Scholastic will immediately investigate, take steps to mitigate the breach and notify the participating educational agency in the most expedient way possible and without unreasonable delay (no later than 7 calendar days after the discovery of the breach). Scholastic will cooperate with the participating educational agency and law enforcement to protect the integrity of investigations into the breach. If the breach is due to the act or omission of Scholastic or its subcontractor or service provider, Scholastic will pay or reimburse the participating educational agency for the full cost of legally-required breach notifications.

9. Without limitation of anything contained in the Addendum, when a subscription period for any digital application ends and subject to applicable law and any other specific terms agreed by contract with the school customer, and without limitation of any “self-service” data deletion tools available in the applicable product, Scholastic retains Protected Data collected in connection with the product until the school customer provides written instructions on renewal and/or data disposition. If Scholastic receives no such instructions, student data will be retained and deleted in accordance with Scholastic’s standard data retention and deletion policies.

10. Subject to any other specific terms agreed by contract with the school customer, at any time a customer may request the deletion of Protected Data, which must be provided in writing (mail or email) to Scholastic either through its customer service team or another Scholastic account representative. Scholastic reserves the right to require verification of identity and confirmation of any necessary consents. Once the deletion is complete Scholastic will provide confirmation in writing if required by the customer. Deletion may take the form of overwriting, pseudonymization or irreversible de-identification to the extent permitted by law.

EXHIBIT D.2 – NIST CSF TABLE

Providers should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, Provider may: (i) Demonstrate alignment using the National Cybersecurity Review ("NCSR") Maturity Scale of 1-7; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

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.	We maintain an up-to-date inventory of technology assets, clarify ownership, and responsibilities for the protection of assets. An enterprise Configuration Management Database is maintained and regularly updated to maintain currency of the information, classify assets according to their criticality and impact on business operations to focus
	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.	Scholastic has established and communicated management structures to convey our mission and objectives and stakeholder commitments. Objectives are clarified and performance managed across all levels of the organization. Vendor risk assessments are conducted and contractual obligations imposed to ensure that vendors and partners meet the Company's privacy and security requirements.
	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.	Scholastic has governance processes in place up to and including Board level oversight of risk levels, completeness, and effectiveness of controls. Scholastic uses internal and external audit functions to evaluate the design and effectiveness of the security controls employed.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Scholastic operates a formal risk assessment process that regularly evaluates risks to enterprise assets, considering a variety of impact factors. Risks are identified for treatment, mitigation, or acceptance. Risk levels are communicated to executive leadership, along with residual risk for further decision-making and management of risk.
	Risk Management Strategy (ID.RM): The organization's	The risk management program focuses on identifying and prioritizing risks based on the Company's business objectives and

	<p>priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>	<p>risk tolerance. The potential impact of threats on critical assets and processes are identified, establishing a risk-aware culture, and implementing policies to manage and mitigate identified risks. Regular reviews ensure that risk management activities are updated to reflect changes in the threat landscape and organizational priorities, enhancing overall resilience. As noted above, risks, mitigations, and residual risk are communicated to executive leadership for regular review and decision-making.</p>
	<p>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.</p>	<p>Vendor risk assessment and management practices are defined and followed for vendor selection and on a regular basis, examining fit for purpose, service delivery, business viability, security, privacy and supporting audit and compliance functions.</p>
<p>PROTECT (PR)</p>	<p>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.</p>	<p>Logical and physical access to systems, data, and facilities is restricted to authorized users. Controls include definition and assignment of roles on a least-privilege basis, management approval of access, regular access review, prompt revocation of access in the event of a job termination or change, maintaining access logs for review, and MFA and SSO for enterprise and high-value assets.</p>
	<p>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.</p>	<p>Scholastic conducts regular and required security awareness training for all employees. Specialized training is conducted for operational staff to ensure responsibilities and processes for handling service and security incidents is also regularly conducted. Information security policies are established and communicated to employees, along with specialized policies for the protection of educational data.</p> <p>Education Solutions staff also receive regular training on privacy, specific to child and student data privacy, including updates on relevant regulations.</p>
	<p>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.</p>	<p>Security controls for data are defined within the corporate information security policy with data classification definitions and required security and handling measures for data based on classification and risk. Data protection includes encryption using generally accepted or better algorithms and cipher length (TLS 1.2, 1.3, AES-256) for sensitive and highly sensitive data.</p>
	<p>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and</p>	<p>Multiple layers of network, infrastructure, and compute layer security are deployed including: network segmentation, next generation firewalls, DDoS protection layers, DNS protection layers, network security groups, intrusion detection,</p>

	<p>coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p>	
	<p>Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p>	<p>Vulnerability disclosure activity is monitored, and operating system and application patching is performed regularly. Scholastic prioritizes timely application of critical patches.</p>
	<p>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.</p>	<p>Proactive security solutions are deployed including network anomaly detection, data loss prevention, vulnerability exploit detection, and reputation-based filtering.</p>
DETECT (DE)	<p>Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.</p>	<p>The SOC operates a SIEM that gathers security event data from across the enterprise including network data, system logs, endpoint activity to analyze, prioritize and drive investigation, mitigation, and remediation of events and incidents.</p>
	<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	<p>The SOC and 24x7 Command Center both operate continuously to monitor and respond to both security and IT events and incidents to maintain security, reliability, and availability commitments to customers and stakeholders. Monitoring and alerting includes traffic and device/service health monitoring and alerting, and synthetic end-user transaction monitoring from multiple geographic locations.</p>
	<p>Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p>	<p>Processes are documented and defined to handle events and alerts and rapidly triage events and escalate as appropriate. Self-healing and high-availability designs and deployments provide built-in safeguards.</p>
	<p>Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</p>	<p>Security incident, technology incident, and data breach response plans are developed, maintained, and followed. Plans define roles and responsibilities, internal and external communications plans, priorities, and escalation paths. Relevant teams train on the plans annually.</p>
	<p>Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).</p>	<p>Internal communication channels with stakeholders are defined and supported by robust tools. Communications with customers and other external stakeholders and entities follow defined responsibilities, also supported by industry standard tools such as status site, CRM, and additional communications as warranted. Notification to customers is provided in accordance with applicable laws and contractual obligations.</p>
	<p>Analysis (RS.AN): Analysis is conducted to ensure effective response and support</p>	<p>Trained staff analyzes events and incidents to define mitigation and remediation approaches, run books and knowledge bases are developed and maintained to aid rapid analysis and recovery.</p>

RESPOND (RS)	recovery activities.	
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	24x7x365 staffing of security and technology operational staff support rapid response to events and incidents. Needed staff and skills are brought to bear to mitigate impact and resolve incidents.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Corrective actions are identified and implemented to help prevent recurrence. Post-incident reviews are conducted which include analysis of the incident to support process, infrastructure, controls, and communications improvements, and identify corrective actions to prevent recurrence. Follow-up actions are formally tracked to resolution.
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.	Business Continuity and Disaster Recovery plans and processes are defined, maintained, and regularly tested to meet security and availability commitments.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Lessons learned from incident response and testing are incorporated into recovery procedures, changes to infrastructure/architecture to improve resilience and service levels.
	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).	Recovery plans include communications procedures, roles, and responsibilities to ensure timely and accurate communication to internal and external stakeholders. Appropriate stakeholder communications tools are deployed to assist in meeting communications objectives.