DATA PRIVACY AGREEMENT

Medina Central School District

and

Scholastic Inc.

This Data Privacy Agreement ("DPA") is by and between the Medina Central School District ("EA"), an Educational Agency, and Scholastic Inc. (including its affiliates, "Contractor"), collectively, the "Parties".

RECITALS

WHEREAS, the Contractor has agreed to provide the EA with certain services ("Services") pursuant to an End User License Agreement dated 7/1/2021 and expires on 6/30/2022 ("Service Agreement"); and

WHEREAS, in order to provide the Services, the Contractor may receive from the EA and the EA may provide the Contractor student data, teacher and/or principal data (collectively, "Personally Identifiable Information" or PII), protected by several New York and federal laws and regulations, among them, the Federal Educational and Privacy rights 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); Education Law § 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the laws referred to above.

NOW THEREFORE, the Parties agree as follows:

ARTICLE I: DEFINITIONS

As used in this agreement, the following terms shall have the following meanings:

1. **Authorized Users:** Contractor's employees and non-employee recipients.
2. **Breach:** The unauthorized acquisition, access, use, or disclosure of PII by or to a person not authorized to acquire, access, use, or receive it.
3. **Commercial or Marketing Purpose:** The sale of student data, teacher or principal data, or its use or disclosure, whether directly or indirectly, to derive a profit, for advertising purposes or to develop, improve or market products or services to students.
4. **Contract, agreement or written agreement**: A binding agreement between an EA and a third-party, which shall include but not be limited to an agreement created in electronic form and signed with an electronic or digital signature or a click wrap agreement that is used with software licenses, downloaded and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.
5. **Disclose**: 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.
6. **Education Record:** An education record as defined in FERPA and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
7. **Educational Agency**: A school district, board of cooperative educational services, school, charter school or the New York State Education Department.
8. **Eligible Student:** A student eighteen years or older.
9. **Encrypt or Encryption**: Methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and such confidential process or key that might enable decryption has not been breached, as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304.
10. **Non-Employee Recipients:** Contractor's nonemployee agents, consultants and/or subcontractors engaged in the provision of Services pursuant to the Service Agreement.
11. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
12. **Parent:** A parent, legal guardian or person in parental relation to the student.
13. **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 as applied to teacher and principal APPR data as defined below.

14. **Release:** Shall have the same meaning as Disclose.
15. **Student:** Any person attending or seeking to enroll in an educational agency.
16. **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, regarding students from the student records of an educational agency.
17. **Teacher or Principal 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.

ARTICLE II: DATA PROTECTION

1. **Purpose.** Contractor is permitted to have access to PII solely and exclusively for the purpose set forth in the Service Agreement as outlined in Exhibit B, the parents' bill of rights for data privacy and security supplemental information. Contractor agrees to hold the PII in strict confidence, and not to disclose it for the benefit of another or for any use or purpose other than for providing the Services. The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this Agreement.
2. **Ownership of PII**. Contractor has no property or licensing rights or claims of ownership to any PII.
3. **Right to Review.** The EA has the right to review Contractor's procedures, practices and controls related to the protection of PII. To that end, upon request, Contractor will make available for review summaries of its policies, procedures, practices and documentation related to the protection of PII. In addition, on reasonable prior written notice, Contractor may be required to undergo an audit of its privacy and security controls performed by an independent third party engaged by Contractor at Contractor's expense (no more frequently than once per 12-month period, except in the case of a breach), and provide a summary of the audit report to EA, or in the alternative, provide EA with a summary of a recent independent audit report on privacy and security controls. Except as otherwise required by law or agreed in writing between the Parties, and excluding PII 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 the Chief Privacy Officer (CPO) of the New York State Education Department and such parties that the EA determines are necessary to assist it in its review and require such other 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.

4. **Parent and Eligible Student Access**. Education Law §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 the Contractor to facilitate such review by a Parent or Eligible Student, and as applicable, 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.
5. **Compliance with Law**. Contractor agrees to maintain the confidentiality of PII in accordance with applicable New York and federal laws, rules, and regulations including, but not limited to, FERPA; COPPA; PPRA; IDEA; Education Law § 2-d; 8 NYCRR Part 121; and EA policies relating to data privacy and security as amended, including, without limitation, those data privacy and security policies that are implemented subsequent to the execution of this DPA and which are provided to Contractor.
6. **Bill of Rights for Data Privacy and Security**. As required by §2-d of the Education Law, the parents' bill of rights for data privacy and security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall sign Exhibit A and complete and sign Exhibit B for the Service Agreement and append it to this DPA. Pursuant to Education Law §2-d, the EA is required to post the completed Exhibit B on its website.
7. **Contractor's Authorized Users**. Contractor shall only disclose PII to Authorized Users who need to know the PII in order to carry out the Services, provided that such disclosure shall be made only to the extent justifiable by such need, and shall adopt and maintain administrative, physical and technical security and privacy controls and protocols that ensure access only to Authorized Users. Contractor shall ensure that all such Authorized Users comply with the terms of this DPA. Contractor agrees that, solely to the extent required by law and subject to any reasonable non-disclosure requirements of Contractor, upon request by the EA, it will provide the EA with the names and affiliations of the Non-Employee Recipients to whom it proposes to disclose, or has disclosed, PII. Contractor shall ensure that each Non-Employee Recipient is contractually bound by an agreement that includes confidentiality and data security obligations equivalent to, and no less protective than, those found in this DPA.
8. **Subcontractor.** Where use of a subcontractor is utilized, Contractor shall, by written agreement, ensure that the applicable requirements set forth herein apply substantively to all subcontractors performing functions pursuant to the Service Agreement where the

subcontractor will receive or have access to PII. Such written agreements shall include provisions that ensure that the subcontractors will abide by all applicable data protection and security requirements, including but not limited to the substance of those requirements included in the Service Agreement, this DPA, and applicable New York and federal laws and regulations. Contractor shall take full responsibility for the acts and omissions of its subcontractors. Contractor shall examine the data security and privacy measures of its subcontractors in accordance with its standard vendor due diligence before it agrees to utilize the subcontractor and shall periodically do so in accordance with its standard vendor management for as long as the subcontractor is being utilized to fulfill the Contractor's responsibilities under the Service Agreement. If at any point a subcontractor fails to comply in any material way with the requirements of this DPA, Contractor shall take such actions as Contractor deems appropriate, that may include: notifying the EA; retrieving all PII received or stored by such subcontractor and ensure that such data has been securely deleted and destroyed in accordance with this DPA; and, remove such subcontractor's access to PII. In the event there is an incident in which the subcontractor compromises PII in a manner that constitutes a Breach as defined in this DPA, Contractor shall promptly notify the EA and follow the Data Breach reporting requirements set forth herein.

9. **Destruction of Data**. Nothing in the Service Agreement shall authorize Contractor to maintain PII after termination of the Service Agreement except as expressly provided herein. At the EA's written request, Contractor shall provide the EA a written certification of the secure deletion and/or destruction and/or irreversible de-identification of PII held by the Contractor and its Non-Employee Recipients no later than sixty (60) business days after the Service Agreement terminates. If applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer, in a format agreed to by the Parties, PII to the EA or the EA's successor contractor at the EA's option, expense (as may be set forth in the Service Agreement) and written direction provided to the Contractor prior to or immediately upon the expiration or termination of the Service Agreement. Contractor shall thereafter, at the EA's written request, with regard to all PII 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 Non-Employee Recipient, securely delete, irreversibly de-identify and/or destroy such PII in a manner that does not allow it to be retrieved or retrievable, read or reconstructed, and direct its Non-Employee Recipients to do the same. Contractor shall ensure that no copy, summary or extract of the PII is retained on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever by Contractor or its Non-Employee Recipients. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise cannot be reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. [Redaction is specifically excluded as a means of data destruction]. Notwithstanding the foregoing, Contractor shall be entitled to retain archive copies required to

be retained by law 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.

10. **No Sale or Commercial Use**. Contractor agrees that it will not sell PII; use or disclose PII for purposes of receiving remuneration, whether directly or indirectly; use or disclose PII for marketing, commercial or advertising purposes (other than to provide the contracted Services to the EA) or facilitate its use or disclosure by any other party for such purposes; or use or disclose PII to develop, improve or market products or services to students, or permit another party to do so.
11. **Disclosure Limitations.** Unless as permitted by this DPA, Contractor shall not disclose any PII to any party who is not an Authorized User. Notwithstanding the foregoing, Contractor may disclose PII if such disclosure is required by statute or court order and the Contractor makes a reasonable effort to notify the EA of the 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 statute or court order.
12. **Encryption.** Contractor shall use appropriate industry standard practices to preserve and protect PII from unauthorized disclosure. Contractor shall use Encryption technologies to protect PII at rest, on file storage, database storage, or on back-up media, and in transit/motion.
13. **Data Security and Privacy Plan**. Contractor shall maintain reasonable administrative, technical and physical safeguards that conform to federal, State and EA mandates, the NIST Cybersecurity Framework or an equivalent standard that meets and or exceeds its requirements, and generally recognized industry standards and practices to protect the security, confidentiality and integrity of PII in its custody. Contractor is required to have a Data Security and Privacy Plan that, at a minimum, complies with 8 NYCRR Part 121, and is acceptable to the EA. Contractor's data privacy and security safeguards are described in greater detail in its' Data Privacy and Security Plan attached hereto as Exhibit C.
14. **Training**. To the extent required by law or regulation, Contactor shall ensure that all Authorized Users who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data and understand their privacy and data security obligations prior to receiving access.
15. **Data Breach Reporting**. Contractor shall immediately notify the EA of any breach of security resulting in an unauthorized release or disclosure of PII by Contractor or its Authorized Users in violation of applicable state or federal law and/or this DPA in the most expedient way possible and without unreasonable delay, but no later than seven (7) calendar days after discovery of the breach or unauthorized release. 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 first class mail, postage prepaid, at the address set forth on Exhibit B. Such notification shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include a brief description of the breach or

unauthorized release; the dates of the incident and the date of discovery, if known; a description of the types of Personally Identifiable Information affected, an estimate of the number of records affected, a brief description of the Contractor's investigation or plan to investigate, and contact information for representatives who can assist the EA. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The breach and unauthorized release of certain Personally Identifiable Information protected by Education Law Section 2-d may subject the Contractor to additional penalties.

16. **Cooperation with Investigations.** Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, to protect the integrity of any investigations into a breach or unauthorized release of PII. 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.
17. **Notification Costs.** Where a breach or unauthorized release of PII occurs that is attributable to Contractor or any of its Authorized Users, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to parents, students, teachers, and/or principals, in accordance Education Law § 2-d and 8 NYCRR Part 121.

ARTICLE III: MISCELLANEOUS

1. **Priority of Agreements and Precedence.** In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein, the Service Agreement, and any of Contractor's terms of service or privacy notices that apply to the Services, the terms and conditions of this DPA shall prevail to the extent of such conflict. In addition, this DPA and all its Exhibits shall be deemed a part of and incorporated into the Service Agreement but shall survive the termination of the Service Agreement in the manner set forth herein.
2. **Entire Agreement**. This DPA constitutes the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.
3. **Governing Law; Venue and Jurisdiction.** This DPA will be governed by and construed in accordance with the laws of the state of New York, without regard to conflicts of law principles. The state and federal courts located in New York will have exclusive jurisdiction to adjudicate any dispute arising out of or relating to this DPA, the Service Agreement referenced in this DPA, or the transactions contemplated hereby.
4. **Execution.** This DPA as well as attached exhibits A, B and C 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. This DPA as well as the attached exhibits A, B and C may be executed by signatures to facsimile copy or electronic transmittal documents in lieu of an original or machine generated or copied document, and each signature thereto shall be and constitute an original signature, as if all Parties had executed a single original document.

SCHOLASTIC INC.

Signature: Toni Abrahams

Printed Name: Toni Abrahams

Title/Position: Vice President

Date: 6/9/2021

MEDINA CENTRAL SCHOOL DISTRICT

Signature:

Printed Name: Anthony S Moreno

Title/Position: Data Protection officer

Date: 6/9/21

EXHIBIT A - EDUCATION LAW §2-D BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Medina 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 cannot be sold or released for any commercial purposes.

2) Parents have the right to inspect and review the complete contents of their child's education record.

3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4) A complete list of all student data elements collected by New York State is available for public review at the following website http://www.nysed.gov/data-privacy-security/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.

5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website http://www.nysed.gov/data-privacy-security/report-improper-disclosure

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Medina Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

1) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

2) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);

3) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);

4) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

5) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and

6) Address how the data will be protected using encryption while in motion and at rest.

SCHOLASTIC INC.

Signature: Toni Abrahams

Printed Name: Toni Abrahams

Title/Position: Vice President

Date: 6/9/2021

EXHIBIT B - BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PII

The Educational Agency is required to post information to its website about its agreements with third-party contractors that will receive PII pursuant to Education Law §2-d and Part 121.3 of the Commissioner's Regulations.

Contact information for notifications of any breach of security resulting in an unauthorized release or disclosure of PII by Contractor or its Authorized Users is as follows:

Medina CSD Data Protection Officer (DPO):

- Name: Anthony Moreno
- Email: amoreno@medinacsd.org
- Phone: 585-798-1534
- Address: 1 Mustang Drive, Medina NY 14103

Name of Vendor	Scholastic Inc.
Products	Scholastic's digital education technology products and digital magazines listed at www.scholastic.com/edtechprivacy.htm, EXCLUDING Scholastic WORD, Scholastic FIRST, and Literacy Pro.
Description of Services	The exclusive purpose for which Contractor uses Student Data is to provide the digital education technology product or services that are the subject of the underlying license agreement. These software products are provided for instructional use in the classroom under the direction of an educator, to support legitimate educational purposes including without limitation promoting literacy.
List of PII Elements	Student Data, which varies depending on the licensed product and the rostering or learning management system used by the EA. Student Data may include full name, student ID, IP address, log-in credentials, school enrollment, metadata on user interaction with the application, grade level, reading level or other performance data, student work, and teacher name associated with the student.

Service Agreement Term (Start and End Dates)	Commences July 1, 2021 and expires on June 30, 2021.
Subcontractors	Contractor will utilize subcontractors in accordance with the terms of the DPA and shall require, pursuant to written agreement, that its subcontractors adhere to the same or greater data protection obligations imposed on the contractor by state and federal laws and regulations, and this DPA.
Data Transition and Secure Destruction	Upon expiration or termination of the contract, at the EA's written request and direction, Contractor shall: ✓ Securely transfer data to EA, or a successor Contractor at the EA's option, expense (as may be set forth in the Service Agreement) and written discretion, in a format agreed to by the parties, ✓ Securely delete, de-identify and/or destroy data, and ✓ Certify to EA that secure deletion is complete.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII may do so by contacting the EA's Data Protection Officer, who will review all such requests. If a correction to data is deemed necessary, Contractor will work with the EA to make such corrections, as applicable.
Secure Storage	PII is stored in Amazon Web Services in the United States. PII is encrypted in motion (currently with TLS 1.2 encryption) and at rest (currently with 128-bit AES encryption). Contractor conducts periodic risk assessments and keep 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 back-ups. Data is classified by sensitivity, and access is rule- and role-based.

Encryption and Data Security	Data will be encrypted while in motion and at rest. Data will be protected with the additional data security and privacy practices outlined in greater detail in Contractor's Data Privacy and Security Plan.

SCHOLASTIC INC.

Signature: Toni Abrahams

Printed Name: Toni Abrahams

Title/Position: Vice President

Date: 6/9/2021

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency is required to ensure that all contracts with a third-party contractor include an acceptable Data Security and Privacy Plan, pursuant to Education Law § 2-d and Part 121.6 of the Commissioner's Regulations. Contractor must complete the following or provide a plan that at a minimum, addresses the following. **While the plan is not required to be posted on the EA's website, contractors should nevertheless ensure that the 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, as consistent with the educational agency's data security and privacy policy.	See attached plan
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect personally identifiable information that you will receive under this contract.	See attached plan
3	Certify compliance with the requirements set forth in the Supplemental Information to the Parents Bill of Rights.	See attached plan
4	Specify how Authorized Users have been trained or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.	See attached plan
5	Outline contracting process that ensures that Authorized users are bound by written agreement to the	See attached plan

	requirements of this DPA, at a minimum.	
6	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 unauthorized disclosures, and to meet your obligations to report incidents to the educational agency.	See attached plan
7	Describe how will data be transitioned to the educational agency when no longer needed by Contractor to provide Services, if applicable.	See attached plan
8	Describe secure destruction practices and how certification will be provided to the educational agency.	See attached plan

SCHOLASTIC INC. DATA SECURITY AND PRIVACY PLAN

In connection with the Data Privacy Agreement (the "DPA") between Scholastic Inc. ("Vendor" or "Scholastic") and Medina Central School District (the "District"), 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 (inclusive of its Supplemental Information requirements), 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 PII subject to New York Education Law Section 2-d and 8 NYCRR Part 121. Any capitalized terms not defined herein shall have the meanings given to them in the DPA.

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 PII as necessary to provide the licensed educational products and services for the benefit of the District, and access to PII 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, PII will be destroyed, returned or de-identified as set forth in the DPA. The term of the license agreement is as indicated in the DPA, order form or similar document entered into by the Parties.
3. Scholastic uses service providers to assist it in performing services for and providing products to educational agencies. Scholastic does not share PII with third parties other than service providers or contractors who are subject to contractual confidentiality and data security obligations, and who may not use the PII for their own purposes. Scholastic ensures that its personnel, service providers and contractors 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 and regulations.
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, DPA or otherwise directed by the educational customer.
6. To protect the security, confidentiality and integrity of protected New York state PII, Scholastic will utilize reasonable administrative, technical, operational and physical safeguards and practices including without limitation the following:
    a. Scholastic stores and processes PII 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 personnel access to PII is further protected by multi-factor authentication and VPN requirements.
    e. Electronic student data is stored in Amazon Web Services.

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 (currently with TLS 1.2 encryption) and at rest (currently with 128-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 PII:

   a. In-person or live remote 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 PII 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 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. 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 PII collected in connection with the application until the school customer provides written instructions on renewal and/or data disposition. In this situation with the District, a DPA has been developed and executed between the Parties that requires a return or destruction of the PII upon expiration or termination of the Service Agreement.

   Subject to any other specific terms agreed by contract with the school customer, at any time a customer may request the deletion of PII, 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 irreversible de-identification to the extent permitted by law.