SCHOLASTIC INC. DATA SECURITY AND PRIVACY PLAN

In connection with the Education Law 2-d Rider (the "Addendum") between Scholastic Inc. ("Vendor" or "Scholastic") and the Bellmore UFSD (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 retains subcontractors 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 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 and subcontractors 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. Student data is stored within the United States 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 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. 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 application until the school customer provides written instructions on renewal and/or data disposition.

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 irreversible de-identification to the extent permitted by law.