



April 28, 2020

RE: Scholastic Inc. Education Technology Products and New York State Education Law Section 2-d and FERPA

To Whom It May Concern:

This letter is in reference to the existing or prospective agreement (the “Agreement”) between you (the “District”) and Scholastic Inc. (“Scholastic” or “Vendor”), for the purchase and/or license of certain print and/or digital educational materials and services from Vendor (the “Program”).

With respect to the digital components of the Program (the “Digital Products”), Vendor acknowledges that any collection, transmission and processing of students’ personally identifiable information via the Digital Products is subject to the provisions of New York State Education Law Section 2-d (“NYS 2-d”) and the Family Educational Rights and Privacy Act (“FERPA”). Such data is referred to in this letter as “Protected Data”.

In recognition of the New York State Department of Education’s goals of promoting the least intrusive data collection policies that advance improved academic achievement, the empowerment of parents, and the enhanced efficiency and effectiveness of schools, as well as the requirements of NYS 2-d, Vendor acknowledges and agrees to the parents’ bill of rights as outlined in NYS 2-d:

- (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 Protected 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 <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentdata.xlsx>, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234; and

- (5) Parents have the right to have complaints about possible breaches of Protected Data addressed.

In furtherance thereof, Vendor shall process Protected Data in accordance with its data security and privacy plan, under which:

- (a) limit internal access to education records to those employees, sub-contractors or service providers that need access to provide the contracted services for legitimate educational interests and not permit any third party to do the same;
- (b) not sell Protected Data or use Protected Data for any purposes (including without limitation marketing) other than providing the Program to the District, or as the District may otherwise authorize;
- (c) ensure that Vendor's personnel who have access to Protected Data have periodic training pertaining to applicable laws and/or industry standards for the confidentiality and security of Protected Data, which training may consist of, without limitation, online interactive courses, in-person trainings, written guidelines, and ongoing advice and counsel from internal and external legal and technical advisors;
- (d) not disclose any Protected Data to any third party (other than sub-contractors or service providers engaged by Vendor pursuant to a written agreement consistent with the parameters of this letter and applicable law) without parental consent except as permitted by applicable law or as explicitly authorized by the District;
- (e) use due diligence and appropriate oversight to ensure that employees, sub-contractors, service providers or other persons or entities that Vendor shares Protected Data with, if any, will abide by applicable data protection and security requirements;
- (f) securely host Protected Data in the United States and use reasonable administrative, technical and physical safeguards, including but not limited to encryption, that align with the NIST Cybersecurity Framework to protect the security, confidentiality and integrity of Protected Data in transit and at rest, and to help prevent access to Protected Data by unauthorized persons;
- (g) at the District's written request (unless otherwise specified in the Agreement and subject to applicable law), return, delete or de-identify Protected Data upon the later to occur of (i) the expiration of the Agreement and (ii) when no longer needed for the benefit of the District, or otherwise according to a schedule that may be agreed on between District and Vendor;
- (h) refer any parental requests to review or correct student records, or any parental inquiries or complaints about possible data breaches, to the District, and cooperate with the District in responding to and resolving such matters on a timely basis consistent with applicable law;
- (i) at the District's written request, provide District with a list of the student data elements collected via the Digital Products;
- (j) enter into any additional data privacy agreement the District may require (including without limitation any District-specific parents' bill of rights) and provide any required supplemental information, subject to good faith negotiation thereof;
- (k) if Scholastic becomes aware of any security breach that results in the unauthorized release of Protected Data in violation of law, the parents' bill of rights, District's policies (to the extent such policies have been communicated to Scholastic in writing) or any contract

- between the parties (a “Security Breach”), immediately investigate such Security Breach and take steps to mitigate the effects thereof;
- (l) notify the District of any Security Breach in the most expedient way possible and without unreasonable delay (no more than seven calendar days after discovery of such Security Breach);
 - (m) cooperate with the District and law enforcement to protect the integrity of investigations into any Security Breach; and
 - (n) where a Security Breach results from the acts or omissions of Vendor or its sub-contractor or service provider, pay for or promptly reimburse the District for the full cost of any required notification to affected individuals.

Scholastic’s privacy policy applicable to Digital Products is available at:
<https://www.scholastic.com/edtechprivacy.htm>.

Please send any data privacy questions to Scholastic at edtechprivacy@scholastic.com. Product-related questions can be emailed to digitalservice@scholastic.com.

Sincerely,

Toni Abrahams

Toni R. Abrahams
VP of Operations
Scholastic Education