Vendor Questionnaire (Data Privacy Agreement): 280221

Created Date: 12/20/2021 3:02 PM Last Updated: 2/28/2022 10:26 AM

Directions

Below is the Third Party contact that will fill out the Part 121//DPA questionnaire. If this is accurate, click the blue "Publish" button. If not, select the appropriate contact by clicking "Lookup" or create a new contact by clicking "Add New".

Vendor Compliance Contacts

Name (Full)	Email	Phone	Third Party Profile
Kathy Brown	kmbrown@scholastic.com		Scholastic
Dennis Slade	dslade@scholastic.com		
Eileen Secchi	esecchi@scholastic.com		
Fred Wolf	fwolf@scholastic.com		
Ian Coughlin	icoughlin@scholastic.com		
Matt Wilcox	mwilcox@scholastic.com		

General Information

Third Party Profile:	Scholastic	**Overall Status:**	Approved
Questionnaire ID:	280221	**Progress Status:**	100%
Engagements:	Scholastic Library Publishing Inc. (DREAM) 22-23	**Portal Status:**	Vendor Submission Received
Due Date:	1/4/2022	**Submit Date:**	2/24/2022
		History Log:	View History Log

Review

Reviewer:	CRB Archer Third Party: Risk Management Team	**Review Status:**	Approved
		Review Date:	2/28/2022
Reviewer Comments:			
Unlock Questions for Updates?:	Assessment questions are set to read-only by default as the assessment should be completed by a vendor through the vendor portal. Do you need to unlock the questionnaire to manually make an update to the submitted questions? This field should be reset to null after the update is made, prior to existing the record.		

Data Privacy Agreement and NYCRR Part 121

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

1. **Breach:** 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. **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.
3. **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.
4. **Education Record:** 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.
5. **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.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **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.
8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **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.
11. **Release:** Shall have the same meaning as Disclose.
12. **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.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **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.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **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.

NYCRR - 121.3 (b)(1):	What is the exclusive purposes for which the student data or teacher or principal data will be used, as defined in the contract?	In providing our Products, we and our service providers may collect the following: Information submitted by a school administrator or teacher about himself or herself, such as first and last name, email address, photo and other profile information, and username and password. Information submitted by a school administrator or teacher about the students in a particular school or classroom, such as first and last names, student ID numbers, usernames and passwords, gender and other demographic information, learning level, and performance data. Sometimes our customer provides us with or permits us to access a school or school district database from which we retrieve this information. We may combine information about a student with information about his or her school, such as its location. Information about a student's parent or guardian, such as names and email addresses. This information may be submitted by a teacher or by the parent or guardian, and we may associate it with the student's information. Information and content submitted by a school

		administrator or teacher, such as lesson plans and notes. Information and content submitted by a student using our Products, such as notes and responses to questions, activities, game play, assessments, assignments, and postings to a bulletin board viewable by others in the same class. Depending on the Product, a student's notes and responses may be provided through open text fields, voice recordings, photographs, or video recordings. If a teacher chooses not to set individual passwords for his or her students' accounts, then students in the same class may be able to access each other's notes or other work. For certain of our Products, the name and email address of an individual to whom a user wishes to send content from the Product. We use the information only to send the message, and we do not retain it. Information about how, where, in a general sense (based on IP address), when, and for how long a user accesses and uses our Products, as well as what content he or she views, what actions he or she takes (including, for example, clicks, touches, and hovers using a mouse), and how he or she navigates through our Products. We may use cookies, pixel tags, and other technologies to collect this information. Information from and about the user's device, such as mobile device type, browser type and version, operating system name and version, IP address, and referring URL. We collect this information automatically when a user accesses our services, to help us understand usage, diagnose problems, administer our Products, and provide support. Information collected through cookies, which are pieces of information stored directly on a user's computer, and other persistent identifiers. We use cookies, IP addresses, and other persistent identifiers to authenticate users in order to ensure that only authorized individuals are permitted access to our Products. Information collected through pixel tags (also known as web beacons and clear GIFs) or other, similar technologies to track how a user navigates through our Products, so that we can understand, for example, what links are clicked and what content is accessed and for how long. This information allows us to improve our user interface and create a better product, such as by making commonly accessed content easier to reach or by more prominently displaying content that has been less frequently accessed. We do not use cookies, pixel tags, or other technologies to track our users' use of third-party services.
NYCRR - 121.3 (b)(2):	Will the organization use subcontractors? If so, how will the organization 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 State and Federal laws and regulations (e.g., FERPA; Education Law section 2-d, NIST Cybersecurity Framework)?	The organization uses a small number of subcontractors in staff augmentation roles. They are embedded within the engineering teams, and are required to take the same regular student privacy and security training as all employees. Identity and access controls for subcontractors is the same as it is for Scholastic employees. Scholastic designs its Products to comply with all applicable laws, including the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA).

NYCRR - 121.3 (b)(3):	What is the duration of the contract including the contract's expected commencement and expiration date? If no contract applies, describe how to terminate the service. Describe what will happen to the student data or teacher or principal data upon expiration. (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be securely destroyed and how all copies of the data that may have been provided to 3rd parties will be securely destroyed)	Contract expires 6/23
NYCRR - 121.3 (b)(4):	How can a parent, student, eligible student, teacher or principal challenge the accuracy of the student data or teacher or principal data that is collected?	Eligible students or their parents or guardians may have the legal right (including under FERPA, COPPA and the California Consumer Privacy Act (CCPA)) to access, correct, export or delete certain of their own information or content, or to make certain choices. To make a request, please contact your school or school district. We will help them provide the requested access or make appropriate corrections. If we receive any such requests directly, we will refer those inquiries to the Education Customer to the extent required or permitted by applicable law or contractual requirements.
NYCRR - 121.3 (b)(5):	Describe where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated.	All SDM data is protected within a secure SDM VPC in AWS. We use industry-standard encryption techniques combined with limited security group access. DevOps and developer access to SDM data is further protected by multi-factor authentication and VPN requirements. No data is stored in "terrestrial" servers. SDM Uses Aurora MySQL RDS database which is encrypted at database level (only available within the SDM VPC, not public). Within our secure VPC in AWS, access to customer information is limited to the few application and devOps engineers who require such access. When engineers leave Scholastic their access to customer information is immediately revoked. To limit access, Scholastic uses AWS security groups, VPNs, and Okta credentialing (with multi-factor authentication). Our applications are multi-tenant. Separation of data between customers is enforced through a common platform shared by all applications. Applications do not have direct database access to customer information, they must use the common platform's APIs to read/write the information. These APIs have permission logic limiting each customer's users to reading/writing only the information belonging to that customer. Student data will be used in aggregate (without PII) for reporting generated by their teachers, principals, or district administrators. Student data is used exclusively by their teachers or principals to record reading levels and assessments. Teacher data is used exclusively by their principals or district administrators to give teachers access to Scholastic products; and to provide principals/administrators information in aggregate reports. No student, eligible student, teacher, or principal data is ever shared with subcontractors or third-party vendors. Production data backups are taken daily and retained for 30 days. After 30 days, data backups are deleted as per AWS RDS standard protocols. At any time a customer may request the deletion of their student, teacher, school, and district data.

NYCRR - 121.3 (b)(6):	Please describe how and where encryption is leveraged to protect sensitive data at rest and while in motion. Please confirm that all encryption algorithms are FIPS 140-2 compliant.	Scholastic bases our controls framework on CIS top 20 and NIST frameworks (CSF and 800-53). We maintain current encryption methodologies using strong keys and these are verified regularly as part of our vulnerabalities scans. We are FIPS 140-2 compliant for all traffic between the end-user and Scholastic. We support TLSv1.2 + and that uses SHA-1. SHA-1 is in the approved list of FIPS compliant protocols. As for at rest, we have encryption enabled in Aurora using AES256.
NYCRR - 121.6 (a):	Please submit the organization's data security and privacy plan that is accepted by the educational agency.	Data Security and Privacy Plan template 11.22.21.pdf
NYCRR - 121.6 (a)(1):	Describe how the organization will implement all State, Federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy.	Our legal, technical, and security teams monitor the regulatory landscape and implement controls and processes aligend to FERPA, COPPA, (and state specific standards on a contract by contract basis
NYCRR - 121.6 (a)(2):	Specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the engagement. If you use 3rd party assessments, please indicate what type of assessments are performed.	All SDM data is protected within a secure SDM VPC in AWS. We use industry-standard encryption techniques combined with limited security group access. DevOps and developer access to SDM data is further protected by multi-factor authentication and VPN requirements. No data is stored in "terrestrial" servers. SDM Uses Aurora MySQL RDS database which is encrypted at database level (only available within the SDM VPC, not public). Within our secure VPC in AWS, access to customer information is limited to the few application and devOps engineers who require such access. When engineers leave Scholastic their access to customer information is immediately revoked. To limit access, Scholastic uses AWS security groups, VPNs, and Okta credentialing (with multi-factor authentication). Our applications are multi-tenant. Separation of data between customers is enforced through a common platform shared by all applications. Applications do not have direct database access to customer information, they must use the common platform's APIs to read/write the information. These APIs have permission logic limiting each customer's users to reading/writing only the information belonging to that customer. Student data will be used in aggregate (without PII) for reporting generated by their teachers, principals, or district administrators. Student data is used exclusively by their teachers or principals to record reading levels and assessments. Teacher data is used exclusively by their principals or district administrators to give teachers access to Scholastic products; and to provide principals/administrators information in aggregate reports. No student, eligible student, teacher, or principal data is ever shared with subcontractors or third-party vendors. Production data backups are taken daily and retained for 30 days. After 30 days, data backups are deleted as per AWS RDS standard protocols. At any time a customer may request the deletion of their student, teacher, school, and district data.
NYCRR - 121.6 (a)(4):	Specify how officers or employees of the organization and its assignees who have access to student data, or teacher or principal data receive or will receive training of the Federal and State laws governing confidentiality of such data prior to receiving access.	All employees must participate in Student Data rights and policies training on an (a minimum) annual basis to ensure we are up-to-date with Federal and State laws.

NYCRR - 121.6 (a)(5):	Specify if the organization will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected.	All contractors, vendors, and consultants are required to review and attest to our corporate information security policy and will adhere to it. They are also required to participate in our security awareness education training (SAE).
NYCRR - 121.6 (a)(6):	Specify how the organization will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency.	There is a defined incident process plan that is followed upon notification of a potential data compromise or breach and notification will be made within 48 hours of confirmation.
NYCRR - 121.6 (a)(7):	Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires. Vendor will be required to complete a Data Destruction Affidavit upon termination of the engagement.	No student, eligible student, teacher, or principal data is ever shared with subcontractors or third-party vendors. Production data backups are taken daily and retained for 30 days. After 30 days, data backups are deleted as per AWS RDS standard protocols. At any time a customer may request the deletion of their student, teacher, school, and district data.
NYCRR - 121.9 (a)(1):	Is your organization compliant with the NIST Cyber Security Framework?	Yes
NYCRR - 121.9 (a)(2):	Describe how the organization will comply with the data security and privacy policy of the educational agency with whom it contracts; Education Law section 2-d; and this Part.	See plan (attached)
NYCRR - 121.9 (a)(3):	Describe how the organization will limit internal access to personally identifiable information to only those employees or sub-contractors that need authorized access to provide services.	Access to any stored protected data is restricted to a limited number of peronnel and managed through role access. The organization uses a small number of subcontractors in staff augmentation roles. They are embedded within the engineering teams, and are required to take the same regular student privacy and security training as all employees. Identity and access controls for subcontractors is the same as it is for Scholastic employees.
NYCRR - 121.9 (a)(4):	Describe how the organization will control access to the protected data and not use the personally identifiable information for any purpose not explicitly authorized in its contract. (e.g. Role Based Access, Continuous System Log Monitoring/Auditing)	Access to any stored protected data is restricted to a limited number of peronnel and managed through role access.
NYCRR - 121.9 (a)(5):	Describe how the organization will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student: (i)except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with State and Federal law, regulations and its contract with the educational agency; or (ii)unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.	We do not disclose any Student Data or Personal Information about the users of our Products to any third party, except: As directed by the Education Customer To our third party service providers, who provide services such as data storage, to permit them to provide those services to us To comply with legal process or respond to governmental requests To protect the rights, safety, or property of Scholastic, our affiliates, our customers, our users or others In connection with certain corporate events such as reorganization, merger, sale or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or other proceeding), in which case the transferred information will remain subject to the terms of this Privacy Policy Our Products do not contain communication tools for students to directly message each other, nor do they enable students to publicly post Student Data. We may use or disclose de-identified, non-personal and aggregate information for any reason, subject to any restrictions imposed by law or our agreement with the Education Customer.

NYCRR - 121.9 (a)(6):	Describe how the organization will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody.	SDM Uses Aurora MySQL RDS database which is encrypted at database level (only available within the SDM VPC, not public). All SDM data is protected within a secure SDM VPC in AWS. We use industry-standard encryption techniques combined with limited security group access. DevOps and developer access to SDM data is further protected by multi-factor authentication and VPN requirements. No data is stored in "terrestrial" servers. Within our secure VPC in AWS, access to customer information is limited to the few application and devOps engineers who require such access. When engineers leave Scholastic their access to customer information is immediately revoked. To limit access, Scholastic uses AWS security groups, VPNs, and Okta credentialing (with multi-factor authentication). At any time a customer may request the deletion of their student, teacher, school and district data.
NYCRR - 121.9 (a)(7):	Describe how the organization will use encryption to protect personally identifiable information in its custody while in motion or at rest.	SDM Uses Aurora MySQL RDS database which is encrypted at database level (only available within the SDM VPC, not public). All SDM data is protected within a secure SDM VPC in AWS. We use industry-standard encryption techniques combined with limited security group access. DevOps and developer access to SDM data is further protected by multi-factor authentication and VPN requirements. No data is stored in "terrestrial" servers.
NYCRR - 121.9 (a)(8):	Affirmatively state that the organization shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.	Affirm
NYCRR - 121.9 (a)(b):	Describe how the organization will supervise its subcontractors to ensure that as subcontractors perform its contractual obligations, the subcontractor will conform with obligations imposed on the third-party contractor by State and Federal law to keep protected data secure.	All subcontractors are supervised by internal Scholastic Management. Security and privacy contract requirements are conveyed to sub-contractors through agreements no less stringent than Scholastic's obligations. Access to any stored protected data is restricted to a limited number of peronnel and managed through role access. The organization uses a small number of subcontractors in staff augmentation roles. They are embedded within the engineering teams, and are required to take the same regular student privacy and security training as all employees. Identity and access controls for subcontractors is the same as it is for Scholastic employees.
NYCRR - 121.10 (a):	Describe how the organization shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach.	The Scholatic security incident management process includes breach notification procedures to our customers.
NYCRR - 121.10 (f):	Affirmatively state that where a breach or unauthorized release is attributed to the organization, the organization shall pay for or promptly reimburse the educational agency for the full cost of such notification.	Affirm
NYCRR - 121.10 (f.2):	Please identify the name of your insurance carrier and the amount of your policy coverage.	Scholastic currently carries $10MM of primary E&O/Cyber Risk with Continental Casualty Company (CNA) and $10MM of excess E&O/Cyber Risk with Mutual Insurance Company for total of $20MM in coverage.

NYCRR - 121.10 (c):	Affirmatively state that the organization will cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.	Affirm
Acceptable Use Policy Agreement:	Do you agree with the Capital Region BOCES Acceptable Use Policy? (Click here: http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&id=BU4QYA6B81BF)	I Agree
Privacy Policy Agreement:	Do you agree with the Capital Region BOCES Privacy Policy? (Click here: http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&id=BWZSQ273BA12)	I Agree
Parent Bill of Rights:	Please upload a signed copy of the Capital Region BOCES Parent Bill of Rights. A copy of the Bill of Rights can be found here: https://www.capitalregionboces.org/wp-content/uploads/2021/03/CRB_Parents_Bill_Of_Rights_-Vendors.pdf	CRB_Parents_Bill_Of_Rights_-Vendors.pdf
DPA Affirmation:	By submitting responses to this Data Privacy Agreement the Contractor agrees to be bound by the terms of this data privacy agreement.	I Agree

Attachments

Name	Size	Type	Upload Date	Downloads
CRB_Parents_Bill_Of_Rights_-Vendors.pdf	258983	.pdf	2/24/2022 1:05 PM	0

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				

Vendor Portal Details

Contact Name:	The Risk Mitigation & Compliance Office	**Publish Date:**	
Required Portal Fields Populated:	Yes	**Contact Email Address:**	crbcontractsoffice@neric.org
About NYCRR Part 121:	In order for a vendor to engage with a New York State Educational Agency, the vendor must provide information required by the New York State Commissioner's Regulations Part 121 (NYCRR Part 121) and the National Institute of Standards and Technology Cyber Security Framework. If deemed appropriate, the responses you provide will be used as part of the data privacy agreement between the vendor and the Albany-Schoharie-Schenectady-Saratoga BOCES. This Data Privacy Agreement ("DPA") is by and between the Albany-Schoharie-Schenectady-Saratoga BOCES ("EA"), an Educational Agency, and Scholastic ("CONTRACTOR"), collectively, the "Parties". 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.	**Requesting Company:**	Capital Region BOCES
Created By:		**Third Party Name:**	Scholastic
		Name:	Scholastic -280221