Vendor Questionnaire (Data Privacy Agreement): 279687
Created Date: 12/6/2021 10:45 AM Last Updated: 1/4/2022 8:50 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
Arlene Riley	arlener@rosenpub.com		Rosen Publishing Group Inc

General Information

Third Party Profile:	Rosen Publishing Group Inc	**Overall Status:**	Approved
Questionnaire ID:	279687	**Progress Status:**	95%
Engagements:	Rosen Publishing Group Inc (DREAM) 22-23	**Portal Status:**	Vendor Submission Received
Due Date:	12/21/2021	**Submit Date:**	1/3/2022
		History Log:	View History Log

Review

Reviewer:	CRB Archer Third Party: Risk Management Team	**Review Status:**	Approved
		Review Date:	1/4/2022
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?	If you become a rostered (adult) user in our Service, we may collect information including name, email address school or district affiliation, phone number, what role you serve at the School, and other identifiable information such as ID numbers, required by the School to use the Service. We store this information in order to fulfill our contractual requirements to deliver contracted services to you. To create accounts, Schools may provide personally identifying information on students, such as first and last name and the class they are assigned to. Students are granted unique usernames and passwords. As students user the Service, we collect information regarding their use of books, activities and games as well as performance data on quizzes, activities, and reading assessments. Wherever we collect student information, we do so in support of the educational purposes such as allowing teachers to review students' work, monitor student performance and progress, and otherwise support instruction. To summarize, the PII collected is solely used to allow us to service LevelUp to the customer.
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)?	Rosen does use third parties to develop and maintain LevelUp. LevelUp has been developed by and is hosted by third parties, but we have agreed with those third parties that they will keep your information secure and not use it for other purposes. We share information with thirdparty service providers only if it is necessary for them to perform services on our behalf in order to support our internal operations.
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)	The term of the contract is July 1, 2021 - June 30, 2022 with two (2) one-year renewals. Upon completion of services, Rosen will remove all PII from its systems within 30 days of the request from the account holder
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?	Challenges to the accuracy of student, teacher or principal data may be submitted to any senior Rosen Customer Service or Professional Development employee by a verifiable adult contact at the institution
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.	LevelUp PII is stored on Amazon Cloud infrastructure. All passwords are encrypted on LevelUp so access is not available to employees. Administrative access to Boces accounts will only be granted to Rosen employees who require it for Rosen's effort to provide our services to you. All data in transit is encrypted using SSL. Our servers have firewalls and other protections in place. These servers are monitored 24/7
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	Passwords at rest are encrypted and all data in transit is encrypted. All encryption algorithms are

	encryption algorithms are FIPS 140-2 compliant.	FIPS 140-2 compliant
NYCRR - 121.6(a):	Please submit the organization's data security and privacy plan that is accepted by the educational agency.	
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.	Rosen has reviewed the policy requirements for data security and privacy as mandated by the New York State and the federal government and designed its policies to meet these requirements as outlined in the sections below. The policies and procedures will remain in place for the life of the agreement
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.	Administrative, operational, and technical safeguards and practices include: Rosen's cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners. Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed. Rosen's organizational cybersecurity policy is established and communicated. Governance and risk management processes address cybersecurity risks (NIST Framework Identify section ID.GV-1–4) Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. Physical access to assets is managed and protected. Remote access is managed. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. Network integrity is protected (e.g., network segregation, network segmentation). Identities are proofed and bound to credentials and asserted in interactions. Users, devices, and other assets are authenticated (e.g., singlefactor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks). (NIST Framework Protect section PR.AC.-1–7) Data-at-rest is protected. Data-in-transit is protected. Assets are formally managed throughout removal, transfers, and disposition. Adequate capacity to ensure availability is maintained. Protections against data leaks are implemented. Integrity checking mechanisms are used to verify software, firmware, and information integrity. The development and testing environment(s) are separate from the production environment. Integrity checking mechanisms are used to verify hardware integrity. (NIST Framework Protect section PR.DS.-1–7) A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality). A System Development Life Cycle to manage systems is implemented. Configuration change control processes are in place. Backups of information are conducted, maintained, and tested. Policy and regulations regarding the physical operating environment for organizational assets are met. (NIST Framework Protect section PR.IP-1–5)
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.	Users are informed and trained on the federal and state laws governing confidentiality of data prior to receiving access. Privileged users understand their roles and responsibilities. Senior executives understand their roles and responsibilities. Physical and cybersecurity personnel understand their roles and responsibilities. (NIST Framework Protect section PR.AT-1, 2, 4, 5)
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.	Third-party stakeholders (e.g., suppliers, customers, partners) are aware of federal and state laws governing the confidentiality of data and understand

		their roles and responsibilities. (NIST Framework Protect section PR.AT-1 merged with 3)
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.	Asset vulnerabilities are identified and documented. Cyber threat intelligence is received from information sharing forums and sources. Threats, both internal and external, are identified and documented. Threats, vulnerabilities, likelihoods, and impacts are used to determine risk. Risk responses are identified and prioritized. (NIST Framework Identify section ID.RA-1, 2, 3, 5, 6) DREAM would be promptly notified. The network is monitored to detect potential cybersecurity events. The physical environment is monitored to detect potential cybersecurity events. Personnel activity is monitored to detect potential cybersecurity events. Malicious code is detected. Unauthorized mobile code is detected. External service provider activity is monitored to detect potential cybersecurity events. Monitoring for unauthorized personnel, connections, devices, and software is performed. Vulnerability scans are performed. (NIST Framework Detect section DE.CM-1–8)
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.	The data will be destroyed 15 to 30 days after the expiration of the agreement. Transfers or delays in destruction of data may be requested within 14 days expiration of the agreement. Destruction may be delayed upon customer request if received prior to the destruction. Rosen's data destruction and transfer policies can be adjusted per agreement terms required by the DREAM Consortium so long as such terms do not conflict with federal and state laws.
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.	Rosen will comply with the policy requirements for data security and privacy as mandated by the educational agency with whom it is contracting and designed its policies to meet these requirements. The policies and procedures will remain in place for the life of the agreement.
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.	Your personal information is stored in data centers controlled by third-party hosting companies and on Rosen premises. The data centers controlled by third-party hosting companies are specifically designed to be physically secure and to only admit authorized personnel who are contractually bound to keep all our data confidential. Access to our customer database is only given to those Rosen employees who need such access in order to carry out the necessary processing of your account
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)	Personal information is stored in data centers controlled by third-party hosting companies and on Rosen premises. The data centers controlled by third-party hosting companies are specifically designed to be physically secure and to only admit authorized personnel who are contractually bound to keep all our data confidential. Access to our customer database is only given to those Rosen employees who need such access in order to carry out the necessary processing of the accounts.
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	Rosen does not sell or or release any student's personally identifiable information for any commercial purposes. Rosen protects the confidentiality of personally identifiable information for students, teachers, and/or principals using safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection. Personally identifiable information is destroyed

	information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.	according to policy once agreement expires. Student, teacher, and principal data will be stored in secured data centers and protected by encryption, firewalls, and password protection. https://www.nysenate.gov/legislation/laws/EDN/ 2-D (section 5.c.1–5
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.	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality). A System Development Life Cycle to manage systems is implemented. Configuration change control processes are in place. Backups of information are conducted, maintained, and tested. Policy and regulations regarding the physical operating environment for organizational assets are met. (NIST Framework Protect section PR.IP-1–5)
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.	Rosen Publishing protects all data in transit using SSL SHA-256 with RSA Encryption. All data at rest is protected by the principle of least privilege
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.	Third-party stakeholders (e.g., suppliers, customers, partners) are aware of federal and state laws governing the confidentiality of data and understand their roles and responsibilities. (NIST Framework Protect section PR.AT-1 merged with 3). Rosen supervises.
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.	Rosen strives to keep to industry-standard security practices. In the unlikely event of a data breach, we will work to remedy said breach. All affected institutions will be notified, and Rosen will support the subscribing institution in their notifying affected individuals, students, and/or families, in compliance with applicable laws.
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.	NFP Property & Casualty Services Inc. Insurer A: Great Northern Insurance Company Insurer B: Federal Insurance Company Commercial General Liability $1,000,000 General Aggregate 2,000,000 Automobile Liability 1,000,000 Umbrella Liability 15,000,000 Workers Comp and Employers Liability 500,000
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	
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
No Records Found				

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 Rosen Publishing Group Inc ("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:**	Rosen Publishing Group Inc
		Name:	Rosen Publishing Group Inc-279687
		Legacy Submit Date:	