Vendor Questionnaire (Data Privacy Agreement): 279680
Created Date: 12/6/2021 10:41 AM Last Updated: 1/3/2022 1:33 PM

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
Mackin Compliance	compliance@mackin.com		Mackin Book Company

General Information

Third Party Profile:	Mackin Book Company	**Overall Status:**	Approved
Questionnaire ID:	279680	**Progress Status:**	100%
Engagements:	Mackin Book Company (DREAM) 22-23	**Portal Status:**	Vendor Submission Received
Due Date:	12/21/2021	**Submit Date:**	12/30/2021
		History Log:	View History Log

Review

Reviewer:	CRB Archer Third Party: Risk Management Team	**Review Status:**	Approved
		Review Date:	1/3/2022
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?	Mackin uses Student Information for the sole purpose of providing user access to and operation of MackinVIA™. Student Information shall mean personally identifiable information of a student and their "education records" as defined in the Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. § 1232g and Personally Identifiable Information as defined in the Children's Online Privacy Protection Act of 1998 (COPPA) 15 U.S.C. § 6501-6506. Student Information shall not include anonymous information which does not enable identification of an individual student, or de-identified information for which all personally identifiable information has been removed and an individual student is not identifiable.
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)?	No sub-contractors will be used.
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 AGREEMENT commences on 07/01/2022 and expires on 06/30/2023. Upon expiration of the AGREEMENT without renewal, or upon termination of the AGREEMENT prior to expiration, Mackin Book Company will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Mackin Book Company or its assignees or subcontractors. If requested by a Participating Educational Agency, Mackin Book Company will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion. At BOCES request, Mackin Book Company will cooperate with BOCES as necessary in order to transition Protected Data to any successor Mackin Book Company prior to deletion. Mackin Book Company agrees that neither it nor its subcontractors, assignees, or other authorized agents will retain any copy, summary or extract of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Mackin Book Company and/or its subcontractors, assignees, or other authorized agents will provide a certification from an appropriate officer that these requirements have been satisfied in full.
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?	Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Mackin Book Company, by contacting the student's district of

		residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Mackin Book Company by following the appeal process in their employing school district's applicable APPR Plan.
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.	Any Protected Data Mackin Book Company receives will be stored on systems maintained by Mackin Book Company, or by a subcontractor under the direct control of Mackin Book Company, in a secure data center facility located within the United States. The measures that Mackin Book Company will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.
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.	Mackin Book Company (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.
NYCRR - 121.6(a):	Please submit the organization's data security and privacy plan that is accepted by the educational agency.	MackinVIA Privacy Policy.pdf MackinVIA Security Plan.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.	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.
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.	Mackin has implemented administrative, physical, and technical infrastructure, as well as procedural safeguards, to protect and maintain the integrity of Student Information. Operating systems and commercial applications are patched to current levels. Critical security patches are deployed within one week of release. Anti-virus software is deployed to all desktops and servers in the Mackin facility and kept up-to-date with the latest definitions. The firewall and DMZ configuration is deployed to prevent public access to Student Information and to segregate that environment from the Internet using a firewall appliance. Only HTTP/HTTPS ports 80 and 443 are allowed through from the Internet to the web server. Third party audits of security operations are conducted quarterly by an approved 3rd party service for compliance with PCI-DSS standards. Mackin is PCI-DSS compliant. For district-initiated security audits, requests may be submitted in writing to Mackin's point of contact.
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.	Mackin Book Company has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Security practices are part of the mandatory employee on-boarding and training program. Access to student data is strictly on a "need-to-know" basis. Access is guarded by an access control list and monitored on network devices.
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.	No sub-contractors will be used.
NYCRR - 121.6(a) (6):	Specify how the organization will manage data security and privacy incidents that implicate personally identifiable information including	In the event that an unauthorized disclosure of Student Information, unauthorized access, or other

	specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency.	incident that threatens the security of Student Information comes to Mackin's attention, the district will be notified immediately. Mackin's Computer Security Incident Response Team (CSIRT) deals with security incidents as recommended by the Handbook for Computer Security Incident Response Teams (CSIRTs), published by the Software Engineering Institute, Carnegie Mellon University. In the case of a security breach, Mackin's CSIRT is trained to: • Make an initial assessment • Communicate the incident • Contain the damage and minimize the risk • Identify the type and severity of the compromise • Protect evidence • Notify external agencies if appropriate • Recover systems • Compile and organize incident documentation • Assess incident damage and cost • Review the response • Update policies
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.	Mackin does not routinely delete stored Student Information unless specifically requested by the district or managing agency. However, Mackin will dispose of or return any Student Information to the district upon request at contract end.
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.	Mackin Book Company will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and BOCES policy on data security and privacy. Mackin Book Company acknowledges that BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, and has provided the policy to Mackin Book Company.
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.	All employees carry key cards that allow access to the building. Each key card is assigned to a specific entrance for a specific time period. Physical access to critical network jacks, wireless access points, gateways, and hand-held devices is restricted. Access to Student Information is strictly on a 'need-to-know' basis. Access to shared Student Information is guarded by an access control list and is monitored on network devices. The identity of all persons having access to Student Information is documented and access is logged. We do not employ external contractors in any capacity unless specific to the contract. Mackin's Privacy Policy is binding upon any external contractor in such cases.
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)	User accounts may be created by the district, end-user, or Mackin. Frequently, the district requests Mackin's assistance with this step. The district has many options for communicating Student Information to Mackin for the creation of Backpack accounts. The information may be shared by automation through LDAP, SIP2, LTI, or SSO; by sending a CSV file of Student Information through Mackin's self-import tool or automated FTP import capabilities; or by sending it in a variety of file formats. Once account setup is complete, any files containing Student Information (not automated) sent to Mackin may be returned to the district, but all copies in Mackin's possession will be destroyed. Automated Student Information uploads are not visible to Mackin employees and are protected by TLS encryption. When transferring Student Information, Mackin appropriates TLS/HTTPS encryption.
NYCRR - 121.9(a) (5):	Describe how the organization will not disclose any personally identifiable information to any other party without the prior written	Mackin collects anonymous information which does not enable identification of an individual student, or

	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.	de-identified information for which all personally identifiable information has been removed and an individual student is not identifiable. This type of information is collected as part of the standard operation of the platform. This may include browser type, operating system, IP address, and the domain name from which the application was accessed. In addition, Mackin may collect information about browsing behavior, such as the date and time of access, the areas or pages visited, the amount of time spent viewing each page, the number of times returned to the application, the referring web page, pages visited, location, mobile carrier, device, and application IDs. Mackin analyzes de-identified, non-personal information and/or aggregated data solely for the purpose of improving service. No information at any point will be transferred or sold.
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.	Mackin has implemented administrative, physical, and technical infrastructure, as well as procedural safeguards, to protect and maintain the integrity of Student Information. Operating systems and commercial applications are patched to current levels. Critical security patches are deployed within one week of release. Anti-virus software is deployed to all desktops and servers in the Mackin facility and kept up-to-date with the latest definitions. The firewall and DMZ configuration is deployed to prevent public access to Student Information and to segregate that environment from the Internet using a firewall appliance. Only HTTP/HTTPS ports 80 and 443 are allowed through from the Internet to the web server. Third party audits of security operations are conducted quarterly by an approved 3rd party service for compliance with PCI-DSS standards. Mackin is PCI-DSS compliant. For district-initiated security audits, requests may be submitted in writing to Mackin’s point of contact.
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.	Using 256-bit AES keys for eBooks and 128-bit or greater AES keys for digital audiobooks, DRM is applied to all titles prior to moving them onto our production server. WAN access to each DRM protected title is limited to authenticated users who have currently “checked out” a copy of that title. All data is transmitted via https.
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.	No sub-contractors will be used.
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.	In the event that an unauthorized disclosure of Student Information, unauthorized access, or other incident that threatens the security of Student Information comes to Mackin’s attention, the district will be notified immediately. Mackin’s Computer Security Incident Response Team (CSIRT) deals with security incidents as recommended by the Handbook for Computer Security Incident Response Teams (CSIRTs), published by the Software Engineering Institute, Carnegie Mellon University. In the case of a security breach, Mackin’s CSIRT is trained to: • Make an initial assessment • Communicate the incident • Contain the damage and minimize the risk • Identify the type and severity of the compromise • Protect evidence • Notify external agencies if appropriate • Recover systems • Compile and organize incident documentation • Assess incident damage and cost • Review the response • Update policies By submitting a written

		request to Mackin's point of contact, in regards to incident investigation, schools may request log data for end user, administrative, and maintenance activity. Mackin carries cyber liability insurance to cover Crisis Management and Computer System Extortion, Media and Content Liability, and Security and Privacy Liability.
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.	Axis Insurance Company $5,000,000
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	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	Yes	**Contact Email**	crbcontractsoffice@neric.org
Fields Populated:		**Address:**	
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 Mackin Book Company ("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:**	Mackin Book Company
		Name:	Mackin Book Company-279680
		Legacy Submit Date:	