


Directions

Below is the Third Party contact that will fill out the Part 121 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
Shaelynn Farnsworth	sfarnsworth@newslit.org		The News Literacy Project

General Information

Third Party Profile:	The News Literacy Project	Overall Status:	Approved
Questionnaire ID:	288132	Progress Status:	 100%
Engagements:	The News Literacy Project Amendment 22-23	Portal Status:	Vendor Submission Received
Due Date:	4/28/2022	Submit Date:	5/31/2022
		History Log:	View History Log

Review

Reviewer:	CRB Archer Third Party: Risk Management Team	Review Status:	Approved
		Review Date:	5/31/2022
Reviewer Comments:			

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.

<p>NYCRR - 121.3 (b)(1):</p>	<p>What is the exclusive purposes for which the student data or teacher or principal data will be used, as defined in the contract?</p>	<p>Collection and encrypted storage of personally identifiable information (PII) for students and teachers is kept to an absolute minimum for viable usage of the product.</p>
<p>NYCRR - 121.3 (b)(2):</p>	<p>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)?</p>	<p>The News Literacy Project has a subcontractor who develops and maintains Checkology virtual classroom. All NLP employees and subcontractors go through yearly training on federal, state, and local guidelines. Along with training, weekly meetings in which data protection and security requirements are addressed, and yearly audits and updates. Regular review of data protection and security requirements throughout the year scheduled.</p>

<p>NYCRR - 121.3 (b)(3):</p>	<p>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)</p>	<p>NLP deletes the personal information about students who use the Checkology® Platform every twelve (12) months. If we are contacted by a parent/guardian for account removal or a contractual relationship ends before the twelve (12)month time period, personal information about students will be deleted. Upon request, data is returned to districts or educational agency up to industry standards.</p>
<p>NYCRR - 121.3 (b)(4):</p>	<p>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?</p>	<p>A parent, student, eligible student, teacher or principal can challenge the accuracy of the student data or teacher or principal data that is collected by written request to Shaelynn Farnsworth, Senior Director of Education Partnership Strategy, sfarnsworth@newselit.org</p>
<p>NYCRR - 121.3 (b)(5):</p>	<p>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.</p>	<p>Checkology is currently hosted on AWS EC2 instances. All PII is encrypted with OpenSSL to provide a minimum of AES-256 encryption. All encrypted values are signed using a message authentication code (MAC) so that their underlying value cannot be modified once encrypted. Encrypted PII is only decryptable by the teacher(s) leading a student's section/class. Access to decryption keys are limited on Checkology's servers to the Checkology app itself and a root user (whose login is limited to SSH from identified administrators and is logged). In addition to the application encryption, all system storage is encrypted by Amazon Web Services (AWS) at rest using a combination of industry-standard hardware and software encryption techniques.</p>
<p>NYCRR - 121.3 (b)(6):</p>	<p>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.</p>	<p>Checkology is currently hosted on AWS EC2 instances. All PII is encrypted with OpenSSL to provide a minimum of AES-256 encryption. All encrypted values are signed using a message authentication code (MAC) so that their underlying value cannot be modified once encrypted. Encrypted PII is only decryptable by the teacher(s) leading a student's section/class. Access to decryption keys are limited on Checkology's servers to the Checkology app itself and a root user (whose login is limited to SSH from identified administrators and is logged). In addition to the application encryption, all system storage is encrypted by Amazon Web Services (AWS) at rest using a combination of industry-standard hardware and software encryption techniques.</p>
<p>NYCRR - 121.6 (a):</p>	<p>Please submit the organization's data security and privacy plan that is accepted by the educational agency.</p>	<p>CheckologyPrivacyPledge_Final10142020docx [63748].pdf</p>
<p>NYCRR - 121.6 (a)(1):</p>	<p>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.</p>	<p>The News Literacy Project has a subcontractor who develops and maintains Checkology virtual classroom. All NLP employees and subcontractors go through yearly training on federal, state, and local guidelines. Along with training, weekly meetings in which data protection and security requirements are addressed, and yearly audits and updates to the privacy policy and regulations. Regular review of data protection and security requirements throughout the year scheduled.</p>

<p>NYCRR - 121.6 (a)(2):</p>	<p>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.</p>	<p>Limited access to the platform for only essential NLP employees who must review the privacy policy manual and yearly training/reviews aligned to Federal, State, and local guidelines.</p>
<p>NYCRR - 121.6 (a)(4):</p>	<p>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.</p>	<p>NLP employees who have access to student data, or teacher or principal data receive training on the Federal and State laws governing the confidentiality of such data prior to receiving access. Yearly training, webinars, and certificates are obtained and kept on file.</p>
<p>NYCRR - 121.6 (a)(5):</p>	<p>Specify if the organization will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected.</p>	<p>The News Literacy Project has a subcontractor who develops and maintains Checkology virtual classroom. All NLP employees and subcontractors go through yearly training on federal, state, and local guidelines. Along with training, weekly meetings in which data protection and security requirements are addressed, and yearly audits and updates. Regular review of data protection and security requirements throughout the year scheduled.</p>
<p>NYCRR - 121.6 (a)(6):</p>	<p>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.</p>	<p>NLP shall promptly notify BOCES of any breach or unauthorized release of ProtectedData in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after NLP has discovered or been informed of the breach or unauthorized release. (b) NLP will provide such notification to BOCES by contacting the BOCES Data Privacy Officer, at michele.jones@neric.org. (c) NLP will cooperate with BOCES and provide as much information as possible directly to the Data Protection Officer (DPO) or designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date NLP discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the NLP has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for NLP representatives who can assist affected individuals that may have additional questions. Page 5of 8(d) NLP acknowledges that upon initial notification from subcontractor, BOCES, as the educational agency with which NLP contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department (“CPO”). NLP shall not provide this notification to the CPO directly. In the event the CPO contacts NLP directly or requests more information from NLP regarding the incident after having been initially informed of the incident by BOCES, NLP will promptly inform the Data Protection Officer or designees. (e) NLP will consult directly with the Data Protection Officer or designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.</p>

<p>NYCRR - 121.6 (a)(7):</p>	<p>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.</p>	<p>Within 30 days of the request, data will be returned to the educational agency sing STFP. Additionally, NLP deletes the personal information about students who use the Checkology® Platform every twelve (12) months.</p>
<p>NYCRR - 121.9 (a)(1):</p>	<p>Is your organization compliant with the NIST Cyber Security Framework?</p>	<p>Yes</p>
<p>NYCRR - 121.9 (a)(2):</p>	<p>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.</p>	<p>NLP acknowledges that the Protected Data it receives pursuant to the AGREEMENT may originate from several Participating Educational Agencies located across New York State and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates. (b) NLP 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. NLP acknowledges that BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, and has provided the policy to NLP.</p>
<p>NYCRR - 121.9 (a)(3):</p>	<p>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.</p>	<p>NLP will limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist NLP in fulfilling one or more of its obligations. All authorized employees will have yearly training.</p>
<p>NYCRR - 121.9 (a)(4):</p>	<p>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)</p>	<p>NLP will use Based Access and only grant authorization to essential employees.</p>
<p>NYCRR - 121.9 (a)(5):</p>	<p>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.</p>	<p>NLP will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student and agree to the terms listed.</p>

<p>NYCRR - 121.9 (a)(6):</p>	<p>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.</p>	<p>Collection and encrypted storage of personally identifiable information (PII) for students and teachers is kept to an absolute minimum for viable usage of the product. Collected information includes:•First Name•Last Name•Email Address (not required for students)•School & DistrictName•Teacher & Class Section(Roster Data)•Grade Level•Student ID(Optional when using Roster Data) All PII is encrypted with Open SSL to provide a minimum of AES-256encryption. All encrypted values are signed using a message authentication code (MAC) so that their underlying value cannot be modified once encrypted. Encrypted PII is only decryptable by the teacher(s) leading a student's section/class. Access to decryption keys is limited on Checkology's servers to the Checkology app and a root user (whose login is limited to SSH from identified administrators and is logged).In addition to the application encryption, all system storage is encrypted by Amazon Web Services(AWS)at rest using a combination of industry-standard hardware and software encryption techniques. All data is encrypted in rest and in transit.</p>
<p>NYCRR - 121.9 (a)(7):</p>	<p>Describe how the organization will use encryption to protect personally identifiable information in its custody while in motion or at rest.</p>	<p>All PII is encrypted with Open SSL to provide a minimum of AES-256encryption. All encrypted values are signed using a message authentication code (MAC) so that their underlying value cannot be modified once encrypted. Encrypted PII is only decryptable by the teacher(s) leading a student's section/class. Access to decryption keys is limited on Checkology's servers to the Checkology app and a root user (whose login is limited to SSH from identified administrators and is logged).In addition to the application encryption, all system storage is encrypted by Amazon Web Services(AWS)at rest using a combination of industry-standard hardware and software encryption techniques. All data is encrypted in rest and in transit.</p>
<p>NYCRR - 121.9 (a)(8):</p>	<p>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.</p>	<p>Affirm</p>
<p>NYCRR - 121.9 (a)(b):</p>	<p>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.</p>	<p>Annual audits and weekly meetings for compliance.</p>

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.	NLP shall promptly notify BOCES of any breach or unauthorized release of ProtectedData in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after NLP has discovered or been informed of the breach or unauthorized release. (b) NLP will provide such notification to BOCES by contacting the BOCES Data Privacy Officer, at michele.jones@neric.org. (c) NLP will cooperate with BOCES and provide as much information as possible directly to the Data Protection Officer (DPO) or designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date NLP discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the NLP has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for NLP representatives who can assist affected individuals that may have additional questions. Page 5of 8(d) NLP acknowledges that upon initial notification from the subcontractor, BOCES, as the educational agency with which NLP contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department (“CPO”). NLP shall not provide this notification to the CPO directly. In the event the CPO contacts NLP directly or requests more information from NLP regarding the incident after having been initially informed of the incident by BOCES, NLP will promptly inform the Data Protection Officer or designees. (e) NLP will consult directly with the Data Protection Officer or designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.
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.	Philadelphia Insurance Company - \$2 million in Network Security & Privacy Liability
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=B U4QYA6B81BF)	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=B WZSQ273BA12)	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_-VendorsSF.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
CheckologyOverviewDataFAQ_2022.pdf	1421774	.pdf	5/30/2022 8:00 PM	0

Comments				
Question Name	Submitter	Date	Comment	Attachment
No Records Found				

Vendor Portal Details	
Contact Name:	The Risk Mitigation & Compliance Office
Required Portal Fields Populated:	Yes
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 The News Literacy Project ("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.
Created By:	
Publish Date:	
Contact Email Address:	crbcontractsoffice@neric.org
Requesting Company:	Capital Region BOCES
Third Party Name:	The News Literacy Project
Name:	The News Literacy Project-288132