


**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
Benjamin Bickham	bbickham@edgedocllc.com	317-396-9012	Edge Document Solutions, LLC

**General Information**

<b>Third Party Profile:</b>	Edge Document Solutions, LLC	<b>Overall Status:</b>	Approved
<b>Questionnaire ID:</b>	306354	<b>Progress Status:</b>	 100%
<b>Engagements:</b>	EDGE Document Solutions 23 - 24 Agreement	<b>Portal Status:</b>	Vendor Submission Received
<b>Due Date:</b>	3/30/2023	<b>Submit Date:</b>	3/29/2023
		<b>History Log:</b>	<a href="#">View History Log</a>

**Review**

<b>Reviewer:</b>	CRB Archer Third Party: Risk Management Team	<b>Review Status:</b>	Approved
		<b>Review Date:</b>	3/31/2023
<b>Reviewer Comments:</b>			

**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><b>NYCRR - 121.3 (b)(1):</b></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>The exclusive purpose for which Vendor (EDGE Document Solutions, LLC) is being provided access to Protected Data is to provide BOCES, the participating educational agency, with print &amp; mail services for New York state test score production and disbursement to parents. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the contract. Protected Data received by Vendor, or any of Vendor’s subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.</p>
<p><b>NYCRR - 121.3 (b)(2):</b></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>No subcontractors currently have access to Protected data.</p>

<p><b>NYCRR - 121.3 (b)(3):</b></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>July 1, 2023-June 30, 2024. Upon completion of the contracted work, usually within 30 days of completion of the project, Vendor will securely delete or otherwise destroy all Protected Data at rest remaining in the possession of Vendor. If requested by the BOCES, Vendor will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion.</p>
<p><b>NYCRR - 121.3 (b)(4):</b></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>Parents or eligible students can challenge the accuracy of any Protected Data provided by a BOCES to the Vendor, 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 Vendor by following the appeal process in their employing school district's applicable APPR Plan.</p>
<p><b>NYCRR - 121.3 (b)(5):</b></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>Any protected data that Vendor receives will be stored on systems maintained by Vendor in a secure data center facility located within the United States. The measures that Vendor 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.</p>
<p><b>NYCRR - 121.3 (b)(6):</b></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>Encrypted files are received by BOCES using SFTP. Sensitive data at rest is securely deleted within 30 days of completion of the annual processing of test score printing. Encryption algorithms are FIPS 140-2 compliant.</p>
<p><b>NYCRR - 121.6 (a):</b></p>	<p>Please submit the organization's data security and privacy plan that is accepted by the educational agency.</p>	<p>Data Privacy and Security Plan 2023-2024.pdf</p>
<p><b>NYCRR - 121.6 (a)(1):</b></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>Files are received from authorized personnel at BOCES for print production and are only handled by two authorized people at Vendor's location who have received training on FERPA, HIPPA, and other protocols in handling PII data. Files will be held on a secure server located within the United States during the time the production is needed.</p> <p>Once test score files have been processed and mailed/shipped to parents and/or schools, files are deleted to prevent duplication.</p>

<p><b>NYCRR - 121.6 (a)(2):</b></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>Vendor follows the principle of least privilege. Access to sensitive information is only granted to the personnel and/or entities that have legitimate need.</p> <p>Externally, access is only granted to the BOCES representative responsible for providing the needed test score files for processing. All processing is done in house and is not touched by an external party.</p> <p>Vendor has instituted penetration testing against NIST standards to prevent unauthorized access from outside servers.</p>
<p><b>NYCRR - 121.6 (a)(4):</b></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>Officers and employees undergo regular training/testing of HIPAA, FERPA, and other related Federal and State laws through a program called Compliance PhD.</p>
<p><b>NYCRR - 121.6 (a)(5):</b></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>Vendor does not use subcontractors for this service. In the event that a third party would need to be utilized, access would be limited to only the information required to perform the contracted duties.</p>
<p><b>NYCRR - 121.6 (a)(6):</b></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>Vendor shall promptly notify BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay. Vendor will cooperate with the designated BOCES security officer to provide as much information as possible about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor 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 Vendor 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 Vendor representatives who can assist affected individuals that may have additional questions.</p>
<p><b>NYCRR - 121.6 (a)(7):</b></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>Data received from BOCES to Vendor is not typically returned to the BOCES, unless requested. Approximately 30 days after completion of test score printing and mailing, all files in possession of vendor are securely deleted and destroyed. If requested by a Participating Educational Agency, Vendor will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion. Vendor agrees that it will not retain any copy, summary or extract of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor will provide a certification from an appropriate officer that these requirements have been satisfied in full.</p>

<b>NYCRR - 121.9 (a)(1):</b>	Is your organization compliant with the <a href="#">NIST Cyber Security Framework</a> ?	Yes
<b>NYCRR - 121.9 (a)(2):</b>	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.	Vendor has initiated secure protocols for handling the student data in compliances with all valid Education Laws and policies of BOCES. As this is a once-a-year document printing, communications between Vendor and BOCES are constant during this period of printing and mailing the student documents.
<b>NYCRR - 121.9 (a)(3):</b>	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.	Data is received by Vendor from BOCES through a secured portal with credentials allowed to only the necessary authorized personnel who have received training in FERPA, HIPPA, and other required training programs. When printed, all test scores printed are handled through an automated process that involves no viewing of data by live individuals.
<b>NYCRR - 121.9 (a)(4):</b>	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)	Physical access is controlled by locked, alarmed and camera monitored data facilities both internally and by our infrastructure provider (DataBank). Only employees who have need to access PII in the performance of their duties have access. There are no publicly accessible entry points to any data or file servers. Access to PII related data is logged by user and date/time of access.
<b>NYCRR - 121.9 (a)(5):</b>	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.	Vendor's process for creation and mailing of test score results that involve personally identifiable information is a secure process that involves data being received by Vendor, printed by Vendor, inserted into envelopes by Vendor, and mailed by Vendor. At no time is the data handled by a third party until documents are mailed using the United States Postal Service. All data received by BOCES is destroyed upon completion of project.
<b>NYCRR - 121.9 (a)(6):</b>	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.	Any protected data that Vendor receives will be stored on systems that are protected against outside intrusion. Access to these systems is granted to a two individuals that have received proper training in protecting personally identifiable information. Vendor utilizes industry standard encryption methods in all facets of its infrastructure. PII data is stored securely in a secure data center facility located within the United States. The measures that Vendor 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. Facilities in which these computers and servers are located are accessed by only employees of Vendor and only two are authorized access to work on this project.

<b>NYCRR - 121.9 (a)(7):</b>	Describe how the organization will use encryption to protect personally identifiable information in its custody while in motion or at rest.	Vendor utilizes industry standard encryption methods in all facets of its infrastructure, including:  · Server Database-level Encryption  · SSL Required for all web traffic involving access to sensitive data  · Removal of deprecated protocols (e.g., TLS 1.0, 1.1)
<b>NYCRR - 121.9 (a)(8):</b>	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
<b>NYCRR - 121.9 (a)(b):</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.	Currently the vendor uses no subcontractors to perform the tasks required to complete the yearly processing and printing of test score results. If this becomes necessary in the future, all subcontractor personnel that would handle the sensitive data will be required to go through similar testing that Vendor personnel are required for to assure compliance.
<b>NYCRR - 121.10 (a):</b>	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.	Vendor shall promptly notify BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release. Vendor will notify the representative in charge of protected data as well as the student services contact who has provided the data to the Vendor. This is done typically via email.
<b>NYCRR - 121.10 (f):</b>	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
<b>NYCRR - 121.10 (f.2):</b>	Please identify the name of your insurance carrier and the amount of your policy coverage.	Continental Casualty Company.  General Liability coverage - \$1,000,000 per occurrence. \$2,000,000 General Aggregate Limit
<b>NYCRR - 121.10 (c):</b>	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
<b>Acceptable Use Policy Agreement:</b>	Do you agree with the Capital Region BOCES <a href="http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&amp;id=B U4QYA6B81BF">Acceptable Use Policy?</a> (Click here: <a href="http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&amp;id=B U4QYA6B81BF">http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&amp;id=B U4QYA6B81BF</a> )	I Agree
<b>Privacy Policy Agreement:</b>	Do you agree with the Capital Region BOCES <a href="http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&amp;id=B WZSQ273BA12">Privacy Policy?</a> (Click here: <a href="http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&amp;id=B WZSQ273BA12">http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&amp;id=B WZSQ273BA12</a> )	I Agree
<b>Parent Bill of Rights:</b>	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: <a href="https://www.capitalregionboces.org/wp-content/uploads/2021/03/CRB_Parents_Bill_Of_Rights_-Vendors.pdf">https://www.capitalregionboces.org/wp-content/uploads/2021/03/CRB_Parents_Bill_Of_Rights_-Vendors.pdf</a>	CRB_Parents_Bill_Of_Rights_-Vendors.pdf

**DPA Affirmation:** By submitting responses to this Data Privacy Agreement the Contractor I Agree agrees to be bound by the terms of this data privacy agreement.

Attachments				
Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments				
Question Name	Submitter	Date	Comment	Attachment
No Records Found				

Vendor Portal Details			
<b>Contact Name:</b>	The Risk Mitigation & Compliance Office	<b>Publish Date:</b>	
<b>Required Portal Fields Populated:</b>	Yes	<b>Contact Email Address:</b>	crbcontractsoffice@neric.org
<b>About NYCRR Part 121:</b>	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 Edge Document Solutions, LLC ("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.	<b>Requesting Company:</b>	Capital Region BOCES
<b>Created By:</b>		<b>Third Party Name:</b>	Edge Document Solutions, LLC
		<b>Name:</b>	Edge Document Solutions, LLC-306354