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
Peter Clifford	pclifford@benchmarkeducation.com		Benchmark Education Company LLC
Dan Horton	dhorton@benchmarkeducation.com		

General Information

Third Party Profile:	Benchmark Education Company LLC	**Overall Status:**	Approved
Questionnaire ID:	280218	**Progress Status:**	100%
Engagements:	Benchmark Education Company LLC (DREAM) 22-23	**Portal Status:**	Vendor Submission Received
Due Date:	1/4/2022	**Submit Date:**	1/31/2022
		History Log:	**View History Log**

Review

Reviewer:	CRB Archer Third Party: Risk Management Team	**Review Status:**	Approved
		Review Date:	2/2/2022
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.

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?	We use information that you provide, the school provides directly or through a third-party affiliated with the school (consistent our status as a "school official" under FERPA), or that we collect, including any personal information, to present the Sites and their contents to you, to provide you notices, and to fulfill any other purpose for which you provide us the information. The information, which as noted above may come from you, your school, or third-party sites affiliated with your school, such as Google, Clever, ClassLink, or similar sites, may also be used to allow students, educators, and school administrators to log into the Sites. We may use educator's email addresses to send important updates, to respond to support and feedback inquiries or requests. Please note that we only use student data for education-related purposes and to improve teaching and learning, as described in more detail here: - Services. We use student-identifiable data provided by schools and/or school districts (including affiliated third-parties, such as Google, Clever, or ClassLink) to make the Sites available to a particular student, and to provide related reports and services to that student's school and school district and its educators and administrators. We may also use the data to improve the Sites' content and effectiveness. - Reporting. Benchmark provides reporting capabilities to its educator customers, and these reports are generated based on usage information. - Account Support. Customers' usage data may also be used on an aggregated basis to allow Benchmark's account management, customer service and tech support teams to provide services that meet the specific needs of our educator customers.
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)?	All staff that interact with applications that store student data are required to complete a FERPA/COPPA training certification program and sign a binding non-disclosure agreement before being granted access to those applications. For more information please reference our Privacy Policy: http://help.benchmarkuniverse.com/bubateacher/Content/Customer%20Support/Privacy%20Policy.htm
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)	We do not retain your personal information for longer than is necessary to provide you with the features and services you have requested. When you request an account be deleted, we remove the data from our servers. At expiration or termination of an agreement, we remove the data within 6 months from the termination date. At any time, you may request that we permanently delete personal information immediately be emailing us at techsupport@benchmarkeducation.com. We do retain aggregated, anonymized information for some of the purposes described above.

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?	If you are a district administrator who has provided us with personal information about your employees or students, you may review, revise or delete that information at any time by logging into your account and accessing your district portal. Deleting student information from your district portal will result in that information also being deleted from our servers. If you are a parent or legal guardian of a minor child, you may also have the right to access certain information about your child. To do so, we request that you contact your school or district, which may access your child's information through their classroom portal.
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.	Benchmark Education follows industry best practices for network and physical security. Records are stored (data at rest) in a secure Amazon Web Services (AWS) environment and are encrypted. Benchmark Education has earned a Data Privacy certification through IMS Global.
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.	Benchmark Education utilizes standard SSL encryption and authentication mechanisms with sha256RSA Signature algorithms, sha256 Signature has algorithms, RSA (2048 Bits) Public Key. - Server Authentication (1.3.6.1.5.5. 7.3.1) - Client Authentication (1.3.6.1.5.5.7.3.2)
NYCRR - 121.6 (a):	Please submit the organization's data security and privacy plan that is accepted by the educational agency.	Benchmark Education Privacy Policy Link.docx
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.	Benchmark Universe is hosted on Amazon Web Services (AWS) secure servers. AWS data centers are ISO 27001 certified. Benchmark Education follows industry best practices for network and physical security. All data is transferred to Benchmark Education and between Benchmark Universe systems using SSL security encryption. Records are Stored (data at rest) in a secure AWS environment and are encrypted. In addition to physical safeguards, Benchmark uses firewall configuration to isolate backend services from direct internet access and ensures only required ports are accessible on internet facing applications. All applications require authenticated sessions. We monitor and respond to error alerts on the application which can indicate attempted attacks. We also employ web application firewalls to block known bad actors and other web-based attacks. Penetration testing is utilized regularly to ensure correct configurations.
NYCRR - 121.6 (a)(2):	Specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the engagement. If you use 3rd party assessments, please indicate what type of assessments are performed.	All data is transferred to Benchmark Education and between Benchmark Universe systems using SSL security encryption. Records are Stored (data at rest) in a secure AWS environment and are encrypted. Benchmark Universe is hosted on Amazon Web Services (AWS) secure servers. AWS data centers are ISO 27001 certified. Benchmark Education team members with access to the hosting environment is strictly limited to Tech Leads, senior Technology leaders (e.g. VP, Software Engineering, Chief of Planning and Infrastructure, and CIO), and DevOps personnel. The number of Benchmark Education employees with access to restricted-use data is limited to those who require access to perform their job requirements.

NYCRR - 121.6 (a)(4):	Specify how officers or employees of the organization and its assignees who have access to student data, or teacher or principal data receive or will receive training of the Federal and State laws governing confidentiality of such data prior to receiving access.	All staff that interact with applications that store student data are required to complete a FERPA/COPPA training certification program and sign a binding non-disclosure agreement before being granted access to those applications.
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.	The number of Benchmark Education employees with access to restricted-use data is limited to those who require access to perform their job requirements. These roles include Technical Support personnel, application developers, and product development staff. All Benchmark Education staff and contractors that interact with applications that store student data are required to complete a FERPA/COPPA training certification program and sign a binding non-disclosure agreement before being granted access to those applications.
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.	In the unlikely event that there is an unauthorized disclosure of PII data, we promptly investigate the incident and provide the district with detailed information regarding any incident including the identity of affected Pupil Records and Users. We monitor and respond to error alerts on the application which can indicate attempted attacks. We also employ web application firewalls to block known bad actors and other web-based attacks. Penetration testing is utilized regularly to ensure correct configurations.
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.	We do not retain your personal information for longer than is necessary to provide you with the features and services you have requested. When you request an account be deleted, we remove the data from our servers. At expiration or termination of an agreement, we remove the data within 6 months from the termination date. At any time, you may request that we permanently delete personal information immediately be emailing us at techsupport@benchmarkeducation.com. We do retain aggregated, anonymized information for some of the purposes described above.
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.	Benchmark Universe is hosted on Amazon Web Services (AWS) secure servers. AWS data centers are ISO 27001 certified. Benchmark Education follows industry best practices for network and physical security. All data is transferred to Benchmark Education and between Benchmark Universe systems using SSL security encryption. Records are Stored (data at rest) in a secure AWS environment and are encrypted. In addition to physical safeguards, Benchmark uses firewall configuration to isolate backend services from direct internet access and ensures only required ports are accessible on internet facing applications. All applications require authenticated sessions. We monitor and respond to error alerts on the application which can indicate attempted attacks. We also employ web application firewalls to block known bad actors and other web-based attacks. Penetration testing is utilized regularly to ensure correct configurations.

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.	The number of Benchmark Education employees with access to restricted-use data is limited to those who require access to perform their job requirements. These roles include Technical Support personnel, application developers, and product development staff. All Benchmark Education staff and contractors that interact with applications that store student data are required to complete a FERPA/COPPA training certification program and sign a binding non-disclosure agreement before being granted access to those applications.
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)	Benchmark supports role-based access. Role assignments are determined based on the data provided to Benchmark through the data source. In addition to physical safeguards, Benchmark uses firewall configuration to isolate backend services from direct internet access and ensures only required ports are accessible on internet facing applications. All applications require authenticated sessions. We monitor and respond to error alerts on the application which can indicate attempted attacks. We also employ web application firewalls to block known bad actors and other web-based attacks. Penetration testing is utilized regularly to ensure correct configurations.
NYCRR - 121.9 (a)(5):	Describe how the organization will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student: (i)except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with State and Federal law, regulations and its contract with the educational agency; or (ii)unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.	We never sell or rent your information. This includes all information collected, as noted above, including from third-party affiliates, such as Google, Clever, or ClassLink. We will only share your information in the following circumstances: - When we believe in good faith that disclosure of your information is necessary to protect our rights and those of others, to protect your safety or the safety of others, to investigate fraud or to respond to a government, judicial or other legal request or to comply with the law. - In connection with an organizational change or dissolution, such as a merger, acquisition, reorganization, bankruptcy, sale or wind down, provided that your information will remain subject to the terms of this Privacy Policy. - We may also use or share certain aggregated, anonymized information with a third-party provider to help us analyze the information.
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.	Benchmark Universe is hosted on Amazon Web Services (AWS) secure servers. AWS data centers are ISO 27001 certified. Benchmark Education follows industry best practices for network and physical security. All data is transferred to Benchmark Education and between Benchmark Universe systems using SSL security encryption. Records are Stored (data at rest) in a secure AWS environment and are encrypted. In addition to physical safeguards, Benchmark uses firewall configuration to isolate backend services from direct internet access and ensures only required ports are accessible on internet facing applications. All applications require authenticated sessions. We monitor and respond to error alerts on the application which can indicate attempted attacks. We also employ web application firewalls to block known bad actors and other web-based attacks. Penetration testing is utilized regularly to ensure correct configurations.

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.	All data is transferred to Benchmark Education and between Benchmark Universe systems using SSL security encryption. Records are Stored (data at rest) in a secure AWS environment and are encrypted. Benchmark Education utilizes standard SSL encryption and authentication mechanisms with sha256RSA Signature algorithms, sha256 Signature has algorithms, RSA (2048 Bits) Public Key. - Server Authentication (1.3.6.1.5.5.7.3.1) - Client Authentication (1.3.6.1.5.5.7.3.2)
NYCRR - 121.9 (a)(8):	Affirmatively state that the organization shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.	Affirm
NYCRR - 121.9 (a)(b):	Describe how the organization will supervise its subcontractors to ensure that as subcontractors perform its contractual obligations, the subcontractor will conform with obligations imposed on the third-party contractor by State and Federal law to keep protected data secure.	All Benchmark Education staff and contractors that interact with applications that store student data are required to complete a FERPA/COPPA training certification program and sign a binding non-disclosure agreement before being granted access to those applications.
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 unlikely event that there is an unauthorized disclosure of PII data, we promptly investigate the incident and provide the district with detailed information regarding any incident including the identity of affected Pupil Records and Users.
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.	Benchmark Education has a $3M Cyber insurance policy with Meridian Risk Management covering, among other things, crisis management, fraud response, public relations, forensic and legal expense, extortion loss, extortion threat reward reimbursement, ransomware loss, social engineering fraud loss and telecommunications theft.
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 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 Benchmark Education Company 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.	**Requesting Company:**	Capital Region BOCES
Created By:		**Third Party Name:**	Benchmark Education Company LLC
		Name:	Benchmark Education Company LLC-280218