Vendor Questionnaire (Data Privacy Agreement): 305641

Created Date: 2/23/2023 10:43 AM Last Updated: 3/7/2023 2:53 PM

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
Connie Ruyter	cruyter@capstonepub.com		Coughlan Companies LLC, dba Capstone

General Information

Third Party Profile:	Coughlan Companies LLC, dba Capstone	**Overall Status:**	Approved
Questionnaire ID:	305641	**Progress Status:**	100%
Engagements:	Coughlan Companies LLC Capstone (DREAM) 23-24	**Portal Status:**	Vendor Submission Received
Due Date:	3/10/2023	**Submit Date:**	3/3/2023
		History Log:	**View History Log**

Review

Reviewer:	CRB Archer Third Party: Risk Management Team	**Review Status:**	Approved
		Review Date:	3/7/2023
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?	PebbleGo Create with Buncee's commitment to data security and privacy, and more specifically, student privacy is evident throughout our platform. We do not require students to submit email, gender, or DOB. We do not collect, sell, rent, or otherwise provide personally identifiable information ("PII") to any third parties for advertising or marketing purposes. PebbleGo Create with Buncee participates in the iKeepSafe COPPA Safe Harbor Certification program, and is a signatory of the Student Privacy Pledge. The purpose of data processing is to allow Contractor to provide the requested Services to the Educational Agency ("EA") and perform the obligations under the Contract. More specifically, the purpose of processing data is to enable school oversight and ensure appropriate structure and interaction within a school account using PebbleGo Create with Buncee. The processing of data enables the interaction, communication, creation and sharing within the classroom/school/district account; allows educators and/or administrators to monitor accounts, set permissions and deliver educational content; allows educators to differentiate and personalize a student's educational experience; and provides the admin-educator-student hierarchy within the account. Contractor requires data capture and use for the following reasons: • To confirm the identity of students and educators/administrators • To provide educational services and content • To allow subscribers to create and manage classes, personalize and differentiate instruction, and monitor and assess student progress • To allow subscribers to monitor and safeguard student welfare • To allow subscribers to set creation and sharing permissions and privacies schoolwide • To inform existing subscribers about feature updates, site maintenance, and programs/initiatives (does not include subaccounts)
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)?	Contractor (Organization) will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract.

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)	An Education Agency ("EA") can send a written request to terminate their subscription to PebbleGo Create with Buncee. Upon expiration or termination of the Contract, Contractor shall securely transfer data to the EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties and/or securely delete and destroy data. All data used for processing will be mapped and securely destroyed.
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, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
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.	PII will be stored using a cloud or infrastructure owned and hosted by a third party. The following preemptive safeguards are in place to identify potential threats, manage vulnerabilities and prevent intrusion: • All security patches are applied routinely • Server access logging is enabled on all servers • Fail2ban (an intrusion prevention software framework that protects servers from brute-force attacks) is installed on all servers and will automatically respond to illegitimate access attempts without intervention from Buncee's engineers • Publicly accessible parameter for database instances is set to No, thereby disallowing any unauthorized access to the database servers • SSH key-based authentication is configured on all servers PebbleGo Create with Buncee serves 100% of its traffic over HTTPS. The HTTPS you see in the URL of your browser means when you go to the website, you're guaranteed to be getting the genuine PebbleGo Create with Buncee website. With HTTPS in place, all interactions with PebbleGo Create with Buncee will be undecipherable by an outside observer. They are unable to read or decode data. HTTPS is the same system that many sensitive websites, like banks, use to secure their traffic. PebbleGo Create with Buncee uses SSL security at the network level to ensure all information is transmitted securely. All content (i.e., photos, video, audio, and other content added to your Buncees) is encrypted at rest. All passwords are encrypted using bcrypt algorithm which is based on the secure blowfish encryption algorithm. Account information is stored in access-controlled data centers operated by industry leading partners with years of experience in large-scale data centers. All user information is stored redundantly and backed up in geographically distributed data centers. We utilize multiple distributed servers to ensure high levels of uptime and to ensure that we can restore availability and access to personal data

		in a timely manner. PebbleGo Create with Buncee’s application is hosted on cloud servers managed by Amazon Web Services and Digital Ocean, both of whom have rigorous physical measures to safeguard data, and are compliant with security standards including ISO 27001, SOC 2, PCI DSS Level 1, and FISMA. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. These data centers are staffed 24/7/365 with onsite security to protect against unauthorized entry. Each site has security cameras that monitor both the facility premises as well as each area of the datacenter internally. There are biometric readers for access as well as at least two factor authentication to gain access to the building. Each facility is unmarked so as not to draw any additional attention from the outside and adheres to strict local and federal government standards. Furthermore, physical access to our servers would not allow access to the actual data, as it is all protected via encryption. Data will be encrypted while in motion and at rest.
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.	Organization's data is encrypted in transit and at rest.
NYCRR - 121.6 (a):	Please submit the organization’s data security and privacy plan that is accepted by the educational agency.	Capstone Data Privacy Plan 2022.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.	Throughout the life of the contract, Contractor will: * limit internal access to education records to those individuals that are determined to have legitimate educational interests * not use the education records for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another Third-Party for marketing or commercial purposes * except for authorized representatives of the Contractor to the extend they are carrying out the contract or written agreement, Contractor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student or unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure if expressly prohibited by statute or court order * maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody * use encryption technology to protect data while in motion or in its custody from authorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(h)(2) of Public Law §111-5 * adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework * impose all the terms stated above in writing where the Contractor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Information.

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.	Only those who need it to perform their duties should have access to data Confidential information must be requested from the manager(s) Training and guidance is provided to all employees that will be accessing and handling data (including more specifically, student data) Background checks are performed on all employees NDAs are signed by employees at the start of employment All access to systems and data is revoked upon employment termination When data is stored on paper, employees follow these guidelines: Keep in a locked drawer when not in use Do not leave papers where others could see them Shred and dispose of paper/printouts when no longer needed All data stored electronically is kept secure by taking the following precautions: Use string passwords that should never be shared Data is never be saved to laptops, mobile devices, or removable media Servers are protected by security software and a firewall Backup data frequently Never disclose PII to unauthorized people within or outside of Buncee Data is reviewed, and if no longer required, deleted and disposed of Routinely monitor systems for security breaches and attempts of inappropriate access
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.	Officers and all employees of the Contractor who have access to student, teacher or principal data will receive ongoing training surrounding the Federal and State laws governing confidentiality of the data. This training will be performed and tracked through Curricula.
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.	Yes, contractor will utilize subcontractors. Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract.

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.	The following procedures are in place to manage a data breach: Breach Investigation: Upon discovering a data breach, first and foremost steps are taken to identify the compromised assets and the extent of the breach. A response team consisting of the Director of IT and the Data Privacy Team is created to investigate the breach. Response team will be tasked with isolating the affected systems, including taking the part or the entire site offline. Remediation Efforts: After isolating the damage, review the access logs and the monitoring software to figure out the cause of the breach. Also, consult experts at the cloud hosting service providers to help with the issue. Once the cause is identified, apply and monitor the fix and gradually bring the site online. Response team will also reset all session tokens for its users which will require that they log in again. Access tokens are valid for 24 hours in order to prevent unauthorized access. Internal Communication Plan: If it has been determined a breach occurred, the Director of IT and the Data Privacy Team will inform the President and CFO and explain what is being done to remediate the issue. After a solution has been implemented, an incident report detailing the cause, extent of damage, steps taken and recommendations to avoid in future will be written by the response team and shared internally. Public Notification of Breach: After remediating the issue, the marketing team will work on informing all affected users about the breach and its severity. A brief statement will be shared via email explaining the incident and the solution will be sent within 24 hours after remediation. Additionally, the response team will monitor the dedicated email address security@buncee.com to address any follow-on questions. We have adopted the following backup-and-restore process: Use up-to-date images to spawn new servers. (if applicable also create a new load balancer) Use the latest hot backup of the database to restore user data Update the DNS records to point to the new load balancer Verify the backup-and-restore process was successful

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.	Upon written request of EA, Contractor shall dispose of or delete all Data obtained under the Contract when it is no longer needed for the purpose for which it was obtained, and transfer said data to EA or EA's designee within forty-five (45) business days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Contractor acknowledges EA's obligations regarding retention of governmental data, and shall not destroy Data except as permitted by EA. Nothing in the Contract shall authorize Contractor to maintain Data obtained under the Contract beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Data; (2) Data Destruction; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Contractor shall provide written notification to EA when the Data has been disposed of. The duty to dispose of Data shall not extend to data that has been deidentified or placed in a separate Student account, pursuant to the other terms of the Contract The EA may employ a "Request for Return or Deletion of Data" FORM. Upon receipt of a request from the EA, the Contractor will immediately provide the EA with any specified portion of the Data within forty-five (45) business days of receipt of said request.
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.	Contractor (Organization) will comply with the EA with whom it contracts and Education Law section 2-d by adhering to the following guidelines: * A student's personally identifiable information cannot be sold or released for any commercial purposes * Parents have the right to inspect and review the complete contents of their child's education record * Contractor will follow state and federal laws which 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 will be in place when data is stored or transferred * Contractor will limit internal access to education records to those individuals that are determined to have legitimate educational interests * Except for authorized representatives of the Contractor to the extend they are carrying out the contract or written agreement, Contractor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student or unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure if expressly prohibited by statute or court order * Contractor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody * Contractor will use encryption technology to protect data while in motion or in its custody * Contractor will adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework Contractor has also documented the following information regarding the receipt of student, teacher or principal data: * The exclusive purposes for which the student data or teacher or principal data will be used. * How the Contractor will ensure that the subcontractors, persons or entities that the Contractor will share the student data or teacher or principal data with, will abide by data protection and security requirements. * When the agreement expires and what happens to the student, teacher or principal data upon expiration of the agreement. * If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected. * Where the student, teacher or principal data will be stored, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

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.	Only those who need data to perform their duties have access to data. Prior to accessing data, backgrounds checks and data security training will be performed. Data security training is an ongoing process.
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)	Only those who need data to perform their duties have access to data (role-based access). Prior to accessing data, backgrounds checks and data security training will be performed. Data collection will continuously be monitored to ensure best practices.
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.	Except for authorized representatives of the Contractor to the extend they are carrying out the contract or written agreement, Contractor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student or unless required by statute or court order and the party provides notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure if expressly prohibited by statute or court order
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.	Only those who need it to perform their duties should have access to data Confidential information must be requested from the manager(s) Training and guidance is provided to all employees that will be accessing and handling data (including more specifically, student data) Background checks are performed on all employees NDAs are signed by employees at the start of employment All access to systems and data is revoked upon employment termination When data is stored on paper, employees follow these guidelines: Keep in a locked drawer when not in use Do not leave papers where others could see them Shred and dispose of paper/printouts when no longer needed All data stored electronically is kept secure by taking the following precautions: Use string passwords that should never be shared Servers are protected by security software and a firewall Backup data frequently Never disclose PII to unauthorized people within or outside of Buncee Data is reviewed, and if no longer required, deleted and disposed of Routinely monitor systems for security breaches and attempts of inappropriate access

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.	PebbleGo Create with Buncee serves 100% of its traffic over HTTPS. The HTTPS you see in the URL of your browser means when you go to the website, you're guaranteed to be getting the genuine PebbleGo Create with Buncee website. With HTTPS in place, all interactions with PebbleGo Create with Buncee will be undecipherable by an outside observer. They are unable to read or decode data. HTTPS is the same system that many sensitive websites, like banks, use to secure their traffic. PebbleGo Create with Buncee uses SSL security at the network level to ensure all information is transmitted securely. All content (i.e., photos, video, audio, and other content added to your Buncees) is encrypted at rest. All passwords are encrypted using bcrypt algorithm which is based on the secure blowfish encryption algorithm. Account information is stored in access-controlled data centers operated by industry leading partners with years of experience in large-scale data centers. All user information is stored redundantly and backed up in geographically distributed data centers. We utilize multiple distributed servers to ensure high levels of uptime and to ensure that we can restore availability and access to personal data in a timely manner. PebbleGo Create with Buncee's application is hosted on cloud servers managed by Amazon Web Services and Digital Ocean, both of whom have rigorous physical measures to safeguard data, and are compliant with security standards including ISO 27001, SOC 2, PCI DSS Level 1, and FISMA. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. These data centers are staffed 24/7/365 with onsite security to protect against unauthorized entry. Each site has security cameras that monitor both the facility premises as well as each area of the datacenter internally. There are biometric readers for access as well as at least two factor authentication to gain access to the building. Each facility is unmarked so as not to draw any additional attention from the outside and adheres to strict local and federal government standards. Furthermore, physical access to our servers would not allow access to the actual data, as it is all protected via encryption. Data will be encrypted while in motion and at rest.
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.	The Contractor (Organization) will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract.
NYCRR - 121.10	Describe how the organization shall promptly notify each educational	Within 72 hours of establishing that there was in

(a):	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.	fact a breach, Contractor will notify the point of contact for each educational agency that maintains a contract with Contractor with the following information: Contractor's contact information, the nature of the data breach including the categories and approximate number of users concerned, the likely consequences of the data breach, and the measures taken/proposed to be taken by to address and remedy the data breach. Contractor has implemented the following procedure to manage a data breach: Breach Investigation: Upon discovering a data breach, first and foremost steps are taken to identify the compromised assets and the extent of the breach. A response team consisting of the Director of IT and the Data Privacy Team is created to investigate the breach. Response team will be tasked with isolating the affected systems, including taking the part or the entire site offline. Remediation Efforts: After isolating the damage, review the access logs and the monitoring software to figure out the cause of the breach. Also, consult experts at the cloud hosting service providers to help with the issue. Once the cause is identified, apply and monitor the fix and gradually bring the site online. Response team will also reset all session tokens for its users which will require that they log in again. Access tokens are valid for 24 hours in order to prevent unauthorized access. Internal Communication Plan: If it has been determined a breach occurred, the Director of IT and the Data Privacy Team will inform the President and CFO and explain what is being done to remediate the issue. After a solution has been implemented, an incident report detailing the cause, extent of damage, steps taken and recommendations to avoid in future will be written by the response team and shared internally. Public Notification of Breach: After remediating the issue, the marketing team will work on informing all affected users about the breach and its severity. A brief statement will be shared via email explaining the incident and the solution will be sent within 24 hours after remediation. Additionally, the response team will monitor the dedicated email address security@buncee.com to address any follow-on questions. We have adopted the following backup-and-restore process: Use up-to-date images to spawn new servers. (if applicable also create a new load balancer) Use the latest hot backup of the database to restore user data Update the DNS records to point to the new load balancer Verify the backup-and-restore process was successful

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.	HDI Specialty Insurance Company $3M Coverage. SCYRD25152520000
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	NY_Capital Region BOCES_Law 2d_02102022_All.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
Capstone Data Privacy Plan 2022.pdf	258582	.pdf	3/3/2023 12:15 PM	0
NY_Capital Region BOCES_Law 2d_02102022_All.pdf	310570	.pdf	3/3/2023 12:15 PM	0

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 Coughlan Companies LLC, dba Capstone ("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:**	Coughlan Companies LLC, dba Capstone
		Name:	Coughlan Companies LLC, dba Capstone-305641