Vendor Questionnaire (Data Privacy Agreement): 304180

Created Date: 1/13/2023 2:59 PM Last Updated: 1/30/2023 1:50 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
Lara Kraft	lkraft@infobase.com		Infobase Holdings Inc
Kari Houle	khoule@infobase.com		Infobase Holdings Inc

General Information

Third Party Profile:	Infobase Holdings Inc	**Overall Status:**	Approved
Questionnaire ID:	304180	**Progress Status:**	100%
Engagements:	Infobase Holdings Inc (DREAM) 23-24	**Portal Status:**	Vendor Submission Received
Due Date:	1/28/2023	**Submit Date:**	1/28/2023
		History Log:	View History Log

Review

Reviewer:	CRB Archer Third Party: Risk Management Team	**Review Status:**	Approved
		Review Date:	1/30/2023
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?	The platform does not store or host or manipulate student, teacher or principal data. Data limited to and focused on subscription access controls and Infobase hosted subject content.
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)?	We do use subcontractors and ensure all abide by our data protection and security requirements, including, but not limited to those outlined in applicable state and federal laws and regulations. We will terminate a vendor who cannot comply or restrict access to data shared to meet our agreements using a method of data obfuscation.
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)	Any data received is kept only as long as required to conduct business, typically a year after subscription has ended. Institution can request data be destructed or deidentified sooner by submitting a request to support@infobase.com

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?	by submitting a request to our support team at support@infobase.com
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.	Our products and services are hosted on Amazon Clo methodology for information security and integrity. I www.qualys.com. We also use the AWS suite to mon
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.	Data is encrypted in transit and at rest using industry best practice methods (TLS 1.3 using PKCS #1 SHA-256 with RSA Encryption).
NYCRR - 121.6 (a):	Please submit the organization's data security and privacy plan that is accepted by the educational agency.	Infobase Data Security and Privacy Policy – Admin Portal.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.	We periodically review our procedures and policies to ensure we are complying with regulations or requirements. In addition, employees engage in training at least annually in these areas.
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.	Infobase uses multiple services to ensure our systems We also use the AWS suite of tools to monitor our se we will notify the designated account admins via ema Only internal staff with a validated need to access dat that maintains a separation of duties. A general revie changes roles or status. Infobase does not store or h on subscription access and controls [Account #/Conta authentication and pass an identifier for a generic use https://www.infobase.com/infobase-data-security-a
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.	Only internal staff with a validated need to access dat that maintains a separation of duties. A general revie changes roles or status. Infobase does not store or h on subscription access and controls [Account #/Conta authentication and pass an identifier for a generic use https://www.infobase.com/infobase-data-security-a Infobase conducts training at a minimum annually on
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.	We do use subcontractors and ensure all abide by our data protection and security requirements, including, but not limited to those outlined in applicable state and federal laws and regulations. We will terminate a vendor who cannot comply or restrict access to data shared to meet our agreements using a method of data obfuscation.
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.	An affected client's administrator will be notified by C upon with the client or required by Law.

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.	Any data associated with your subscription to Infobase will be maintained only as long as needed to conduct general business. This is typically 12 months post subscription expiration. Destruction or deidentification of data can be requested before this time bu submitting a request to support@infobase.com.
NYCRR - 121.9 (a)(1):	Is your organization compliant with the NIST Cyber Security Framework?	No
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.	Infobase Data Privacy and Security information can be found here. https://infobaseadmin.zendesk.com/hc/en-us/articles/360007151494-Infobase-Data-Security-and-Privacy-Policy We also regularly review regulations and policies to ensure we are complying with requirements in the education space, including Ed Law 2-d.
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.	We do use subcontractors and ensure all abide by our data protection and security requirements, including, but not limited to those outlined in applicable state and federal laws and regulations. We will terminate a vendor who cannot comply or restrict access to data shared to meet our agreements using a method of data obfuscation.
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)	As a SaaS service that does not host or store student The Infobase family of products do not store or manip email. These fields or the creation of individual users authenticate access is needed to grant access. Since a from our products. The Client can also elect to allow real-world identity when tracking activity is desired th passed and all usage logged as generic id.
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.	The Infobase family of products do not store or manip email. These fields or the creation of individual users authenticate access is needed to grant access. Since a from our products. The Client can also elect to allow real-world identity when tracking activity is desired th passed and all usage logged as generic id.

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 internal staff with a validated need to access dat that maintains a separation of duties. A general revie changes roles or status. Our products and services are hosted on Amazon Clo practices from NIST 800-53 and ISO 27001 standards services to ensure our system and vendor connection We also use the AWS suite to monitor our services ar
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.	Data is encrypted in transit and at rest using industry best practice methods (TLS 1.3 using PKCS #1 SHA-256 with RSA Encryption).
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.	We do use subcontractors and ensure all abide by our data protection and security requirements, including, but not limited to those outlined in applicable state and federal laws and regulations. We will terminate a vendor who cannot comply or restrict access to data shared to meet our agreements using a method of data obfuscation. Only internal staff with a validated need to access dat that maintains a separation of duties. A general revie changes roles or status. Infobase does not store or h on subscription access and controls [Account #/Conta authentication and pass an identifier for a generic use
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.	Infobase will notify the primary contact at the subscribing institution by email of any breach within 24 hours.
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.	Cyber Security Coverage - Endurance American Specialty and Evanston Insurance - $3M/ $100K CGL- StarNet Insurance - $2M/$1M
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	IHI_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

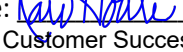
Contact Name:	The Risk Mitigation & Compliance Office	**Publish Date:**	
Required Portal Fields Populated:	Yes	**Contact Email Address:**	crbcontractsoffice@neric.org
About NYCRR Part 121:	In order for a vendor to engage with a New York State Educational Agency, the vendor must provide information required 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 Infobase Holdings Inc ("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:**	Infobase Holdings Inc
		Name:	Infobase Holdings Inc-304180

Parents Bill Of Rights for Vendors Working With Capital Region BOCES

Albany-Schoharie-Schenectady-Saratoga BOCES (Capital Region BOCES), in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. BOCES establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by BOCES or any a third party contractor. BOCES will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by BOCES in accordance with BOCES policy;
- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;
- A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov/data-privacy-security or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the Data Protection Officer, 518-862-5239, DPO@neric.org, Capital Region BOCES, 900 Watervliet-Shaker Rd., Albany NY 12205. Complaints can also be directed to the New York State Education Department online at http://nysed.gov/data-privacy-security by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@mail.nysed.gov or by telephone at 518-474-0937.
- Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.

In the event that BOCES engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the Data Protection Officer, 518-464-5139, DPO@neric.org, 900 Watervliet-Shaker Rd., Albany NY 12205, or can access the information on the Capital Region BOCES website www.capitalregionboces.org.

Vendor/Company Name: Infobase Holdings, Inc.
Signature: 
Title: VP Customer Success & Support
Date: 1/27/2023