Vendor Questionnaire (Data Privacy Agreement): 280710

Created Date: 1/3/2022 1:14 PM Last Updated: 1/19/2022 11:29 AM

Directions

Below is the Third Party contact that will fill out the Part 121//DPA 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
Delfina Manocchio	proposals@careercruising.com		Xello Inc
Imran Khan	imrank@careercruising.com		Xello Inc
Fatima Stepanian	fatimas@careercruising.com		

General Information

Third Party Profile:	Xello Inc	**Overall Status:**	Approved
Questionnaire ID:	280710	**Progress Status:**	100%
Engagements:	Xello Inc (DREAM) 22-23	**Portal Status:**	Vendor Submission Received
Due Date:	1/18/2022	**Submit Date:**	1/14/2022
		History Log:	**View History Log**

Review

Reviewer:	CRB Archer Third Party: Risk Management Team	**Review Status:**	Approved
		Review Date:	1/19/2022
Reviewer Comments:			
Unlock Questions for Updates?:	Assessment questions are set to read-only by default as the assessment should be completed by a vendor through the vendor portal. Do you need to unlock the questionnaire to manually make an update to the submitted questions? This field should be reset to null after the update is made, prior to existing the record.		

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?	Integration of student information.
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)?	Xello does not use subcontractors who have access to student, data or principal data. In the event that this changes, Xello will notify all clients prior to the change.
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)	The duration of the contract is July 1, 2022 through June 30, 2023.

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?	Inaccuracies with student, teacher or principal data can be reported to Xello's support team and/or your Account Manager. Xello will then work with impacted parties to make sure data is corrected in a timely fashion.
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.	Data is stored in Microsoft Azure. Data for US clients is hosted in the US Central region which has datacentres in Iowa. Data is also encrypted both at rest and in transit when moving between the database and the Xello application. All access is limited to Xello employees with a zero trust policy, minimizing access to only users who require it to manage and maintain the application/
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 in Xello is encrypted at rest using Azure Data Encryption, this is regularly monitored to ensure encryption is always available. Xello's also leverages SSL and TLS encryption for data in transit to ensure data is encrypted and only accessible by authenticated users.
NYCRR - 121.6 (a):	Please submit the organization's data security and privacy plan that is accepted by the educational agency.	XELLO - Information Security Policy.pdf XELLO - Privacy Governance Framework and Privacy Policy.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.	Xello ensures we comply with all aspects of data security and privacy. Xello maintains compliance with NY Ed State Law, FERPA, COPPA amongst other legislations. In the event that the client believes Xello does not meet a specific piece of legislation or privacy requirements, these can be raised with your Account Manager or to privacy@xello.world.
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.	Xello has a few security controls in place toe ensure PII is protected at all times: - A robust security and event monitoring tool that alerts Xello of unauthorized attempts or malicious behavior. - Regular review of access to back end systems to ensure zero trust access is maintained. - Automated alerts on data exfiltration or other requests that are outside of typical user behavior. - Data encryption both at rest and in transit. - MFA for Xello administrators to ensure back end access is monitored and maintained. Xello is also in the process of attaining our SOC2 and ISO27001 to further demonstrate our dedication to security and privacy.
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.	Xello provides regular security training that aligns with both best practice and local laws. This is completed an annual basis and done by any users with access to systems that may contain PII.
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.	Xello does not use subcontractors to maintain any systems with PII. Subcontractors or consultants may be used for other organisational needs, however are subject to NDAs and security training similar to that of Xello employees.

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.	Xello's incident management policy means that Xello will ensure that we will notify customers with 48 hours of a discovered breach. This communication may be completed earlier depending on the time required to collect all details regarding the incident. In the event that a customer believes their data may have been breached, they can notify their account manager or privacy@xello.world in order to trigger an investigation.
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.	Following termination or deactivation of a School’s account, we will retain personal information and User Content for a period of 90 days. Should the School decide to renew their contract within this 90-day period, your account and all related information will be restored. At the end of 90 days, or earlier at the request of the School, we will delete or transfer (and direct any subcontractors to delete or transfer) to School with rights in the information: Student Personal Information (including FERPA Records), personal information of Educators, and User Content in our or our subcontractor’s possession. Notwithstanding the foregoing, we may retain any such information as required by or to demonstrate compliance with applicable law. At any time upon termination of an agreement or otherwise at their discretion, School can request we delete all Student Personal Information and User Content. We will follow these instructions within 30 days of receipt.
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.	Xello ensures we maintain compliance with Education Law 2-D by ensuring the following: - PII is not sold or used for marketing purposes. - System monitoring includes data systems monitoring, data encryption , incident response plans, zero trust policy for systems that have PII, destruction of PII when no longer needed. Xello also ensures that in the breach, we would notify impacted agencies in a timely manner.
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.	Xello does not employ subcontractors for the purpose of developing or maintaining Xello, as such they would under no circumstances have access to PII. Internal access is maintained using a zero trust policy — access is only provided to Xello employees who require access to maintain, develop or support the Xello application. Access is regularly reviewed to ensure access no longer required is terminated in a timely manner.
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)	Data is monitored using a security event and monitoring system, this allows Xello to monitor the system for for unauthorized access. Access to the systems are based on organisational roles and a zero trust policy, this access is reviewed regularly to ensure compliance.

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 may permit certain trusted third parties to track usage, as well as analyze information such as the source address that a page request is coming from, your IP address or domain name, the date and time of the page request, the referring website (if any), and other parameters in the URL. This is collected in order to better understand usage of our website and the Services and enhance the performance of and maintain and operate the Services. We may also use trusted third parties to host portions of the Services infrastructure, operate various features of the Services, store content, send emails, and store data on our behalf. We may also disclose personal information in certain special cases, including the following: - We are required to do so by law or as ordered by a court. - To detect, investigate and prevent activities that may be a violation of our Terms of Service or law. - To resolve a technical problem or secure the Services. - As directed by a School or District that has licensed Xello. - We may also share personal information or User Content in connection with a merger, financing, acquisition, bankruptcy, dissolution, transaction, or proceeding involving sale, transfer, divestiture, or disclosure of all or a portion of our business or assets to another company. In these circumstances, we will only share such information with a company that has agreed to data privacy standards no less stringent than our own and after providing advanced notice to you with an opportunity to opt out of our sharing of such information. Third-Party Services Certain third-party products or services (such as single sign on for test preparation services) may be available for schools to choose to integrate within or use within the services. A school is not required to use such additional products in the Services. Before electing to use such third-party services, schools should review the terms, policies and practices of the third-party products and services to understand their terms and policies with respect to any personal information, including student personal information, they may collect. We strive to make available third-party services that will be useful to Schools, but we are not responsible for their practices, including with respect to personal 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.	Xello has a few security controls in place toe ensure PII is protected at all times: - A robust security and event monitoring tool that alerts Xello of unauthorized attempts or malicious behavior. - Regular review of access to back end systems to ensure zero trust access is maintained. - Automated alerts on data exfiltration or other requests that are outside of typical user behavior. - Data encryption both at rest and in transit. - MFA for Xello administrators to ensure back end access is monitored and maintained. Xello is also in the process of attaining our SOC2 and ISO27001 to further demonstrate our dedication to security and privacy.

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 in Xello is encrypted at rest using Azure Data Encryption, this is regularly monitored to ensure encryption is always available. Xello's also leverages SSL and TLS encryption for data in transit to ensure data is encrypted and only accessible by authenticated users.
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.	N/A - Xello does not use subcontractors for the purpose of maintaining or developing the Xello application.
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.	Xello will notify clients by email or via a phone call to the registered administrators of the application. Xello will ensure that any communications are done within 48 hours of a confirmed breach.
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.	Hugh Wood Canada Ltd. Our coverage for commercial general liability is as follows - Per Occurrence – $3,000,000 - General Aggregate Limit – $10,000,000
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	XELLO - 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 Xello 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:**	Xello Inc
		Name:	Xello Inc-280710