


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
Lana Bushell	lana.bushell@clickview.com.au		ClickView
Sam Berry	sam.berry@clickview.com.au		

General Information

Third Party Profile:	ClickView	Overall Status:	Approved
Questionnaire ID:	306265	Progress Status:	
Engagements:	Click View Inc (DREAM) 23-24	Portal Status:	Vendor Submission Received
Due Date:	3/29/2023	Submit Date:	3/20/2023
		History Log:	View History Log

Review

Reviewer:	CRB Archer Third Party: Risk Management Team	Review Status:	Approved
		Review Date:	3/20/2023
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?

ClickView will use student, teacher and principal data solely for educational purposes, as authorized by the BOCES and in compliance with the Contract. Student, teacher and principal data will be used for the sole purpose of access to and use of the product. We do not sell nor use or disclose PII for any marketing or commercial purpose and we do not facilitate the use or disclosure of PII by any other party for marketing or commercial purposes. We will protect the confidentiality of PII in accordance with the Contract and applicable laws and regulations, including the Capital Region BOCES Parent Bill of Rights.

**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 not engage sub-contractors to perform work under the Contract. Sub-contractors who process personal information on our behalf are only engaged to assist us with providing our products. These providers are only granted access to personal information to the extent needed to provide their services for us, strictly in accordance with our instructions, in accordance with applicable privacy laws, our contractual requirements, our contractual obligations to the BOCES and other customers, and not for any commercial purpose. We ensure that sub-contractors that ClickView will share PII with, if any, will abide by data protection and security requirements which are, at a minimum, materially similar and no less protective than the data protection obligations imposed by the BOCES on ClickView.

**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 current request of contract is expected to commence on July 1st 2023 and expire June 30th 2024. Upon expiration of the contract ClickView will securely destroy the data as per our data retention and deletion policy and in accordance with the BOCES requirements.

ClickView will comply with all contractual and legal obligations in connection with the transfer or deletion or destruction of data upon the expiry or termination of the contract.

In particular:

- ClickView will consult with the BOCES in respect of its requirements, including the format of the deletion or transfer;
- ClickView will follow best practice for secure deletion / destruction of data or transfer of data;
- ClickView will certify in writing that data has been surrendered or destroyed in accordance with the BOCES requirements.

**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 a parent, student, teacher or principal seeks a copy of their PII, or seeks to challenge the accuracy of PII in the custody or control of ClickView, ClickView will forward the request to the BOCES as soon as practicable, follow the BOCES instructions on how to process the request, and facilitate any corrections in accordance with ClickView's contractual obligations.

**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 will be stored in secure data center facilities operated by Amazon Web Services (AWS) located within the United States and Australia. AWS's data centres provide industry leading controls to ensure the security of user data stored in their data centres. This includes physical, environmental and infrastructure controls designed to protect the data contained therein

ClickView has and will adopt technologies, safeguards and practices that align with ISO 27001 and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

**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.

ClickView uses AES256 as our encryption standard for data in transit and rest and for backups as well, meaning data is always safely encrypted. All encryptions are FIPS 140-2 compliant.

**NYCRR - 121.6
(a):**

Please submit the organization's data security and privacy plan that is accepted by the educational agency.

ClickView Links.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.

Compliance with law and policy - ClickView will comply with applicable laws and policies, including N.Y. Education Law 2-d and its implementing regulations, the Federal Family Educational Rights and Privacy Act ("FERPA") and the Children's Online Privacy Protection Act ("COPPA"). ClickView will also comply with the Capital Region BOCES Parents' Bill of Rights.

Restrictions on PII use –

- ClickView will use PII solely for educational purposes and as authorized by the BOCES
- ClickView limits internal access to education records to those individuals that are determined to have legitimate educational interests
- Does not use education records for any other purposes than those explicitly authorized in contracts
- ClickView does not sell PII nor use or disclose it for any marketing or commercial purpose and will not facilitate the use or disclosure of PII by any other party for marketing or commercial purposes
- Except for ClickView's authorized representatives and sub-contractors, we will not disclose any PII to any other party without the prior written consent of the parent or eligible student, except as required to carry out the contract, or as otherwise required or permitted by court order or law. We will consult with BOCES if we receive any subpoena, court order or other legal process which relates to PII.

Encryption – we use encryption technology to protect data while in motion and at rest using best practice, as outlined in our Cryptography Policy.

Data privacy and security practices – We will adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework and we will maintain administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in our custody. These safeguards are documented and implemented organizational policies, including our Information Security Policy and Physical and Environment Security Policy.

Data Breach Reporting Obligations – We will Notify the BOCES of any breach or unauthorized release of PII in accordance with our legal and contractual requirements and cooperate with the BOCES and law enforcement in respect of any investigations. Our data breach response process is set out in our Data Breach Response Plan.

<p>NYCRR - 121.6 (a)(2):</p>	<p>Specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the engagement. If you use 3rd party assessments, please indicate what type of assessments are performed.</p>	<p>ClickView takes the security and protection of data very seriously. ClickView is in the process of being independently audited for ISO27001 compliance. ClickView has established a range of policies that address; ISMS, Risk Management, Acceptable Use, Access Control, Asset Management, Information Classification, Change Management, Operations and Communication Management, Physical and environment security, Security Incident Management, Business Continuity, Cryptography, and others aligned to ISO27001 best practice and to the state and government security standards.</p> <p>ClickView has decided to establish, implement and continually improve an Information Security Management System (ISMS) which covers its core IT systems and functions that support the business and address the risk to digital information assets. ISMS provides a systematic approach to managing the security of organization information assets. It encompasses people, processes and IT systems and is based on a risk assessment. Customer data never leaves our secure cloud environment and is not used in local development environments. ClickView uses AES256 as our encryption standard for “in transit” and “at rest” and for backups as well. Appropriate detective, preventative and corrective measures are implemented in information processing facilities and systems to protect against viruses and malicious code. ClickView has been assessed independently by an external firm to run penetration testing and maturity assessments on an annual basis and is continuing to work with them on achieving ISO 27001 compliance.</p>
<p>NYCRR - 121.6 (a)(4):</p>	<p>Specify how officers or employees of the organization and its assignees who have access to student data, or teacher or principal data receive or will receive training of the Federal and State laws governing confidentiality of such data prior to receiving access.</p>	<p>We will conduct training for all new employees who have access to PII and then annually for existing employees.</p>
<p>NYCRR - 121.6 (a)(5):</p>	<p>Specify if the organization will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected.</p>	<p>In the event that ClickView discloses any PII to subcontractors, it will require those subcontractors to comply with substantially the same data security and privacy standards required of ClickView under the Contract and applicable state and federal law.</p> <p>ClickView will oversee the performance of the services by subcontractors to ensure subcontractors are abiding by such standards, and ClickView will undertake reviews and audits where it suspects non-compliance.</p>
<p>NYCRR - 121.6 (a)(6):</p>	<p>Specify how the organization will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency.</p>	<p>ClickView has implemented policies, including a data</p> <p>ClickView’s responses will be compliant with applicab</p> <p>Contacting law enforcement or cyber-crime investiga</p> <p>Our general approach is one of transparency and con</p>

<p>NYCRR - 121.6 (a)(7):</p>	<p>Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires. Vendor will be required to complete a Data Destruction Affidavit upon termination of the engagement.</p>	<p>ClickView will comply with all contractual and legal obligations in connection with the transfer or deletion or destruction of data upon the expiry or termination of the contract. ClickView will facilitate such transfer or deletion or destruction promptly at the BOCES request.</p> <p>At BOCES written request, ClickView will cooperate with BOCES as necessary in order to transition PII to any successor contractor.</p> <p>ClickView will ensure that any subcontractor which holds PII will transfer, delete or destroy such PII in a manner which is consistent with ClickView's process and no subcontractor will retain any PII on any medium whatsoever.</p>
<p>NYCRR - 121.9 (a)(1):</p>	<p>Is your organization compliant with the NIST Cyber Security Framework?</p>	<p>Yes</p>
<p>NYCRR - 121.9 (a)(2):</p>	<p>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.</p>	<p>ClickView will ensure that it complies with the data security and privacy policy of the educational agency with whom it contracts.</p>
<p>NYCRR - 121.9 (a)(3):</p>	<p>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.</p>	<p>ClickView adopts the principle of least privilege access, as outlined in our Access Control Policy. This also includes password policies, MFA, information restriction.</p> <p>Access to production data and servers is restricted by logged separately.</p>
<p>NYCRR - 121.9 (a)(4):</p>	<p>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)</p>	<p>All Users will be required to have a unique logon ID and password for access to systems. The User's password should be kept confidential and must not be shared with management & supervisory personnel or any other users whatsoever.</p> <p>On critical servers and devices, users will not be allowed to logon as a system administrator/privileged user unless required. Users who need this level of access must follow the process to request for special access. The principle of least privilege is observed and privileged access is revoked after access is no longer required.</p> <p>User accounts will be deactivated or removed if the user is terminated, suspended, placed on extended leave, or otherwise leaves the employment of ClickView.</p>

<p>NYCRR - 121.9 (a)(5):</p>	<p>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.</p>	<p>ClickView will use PII solely for educational purposes and as authorized the BOCES. We will not disclose any PII to any other party without the prior written consent of the parent or eligible student, except as required to carry out the contract, or as otherwise required or permitted by law.</p>
<p>NYCRR - 121.9 (a)(6):</p>	<p>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.</p>	<p>ClickView has adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework and we will maintain administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in our custody. This is outlined in a range of implemented policies such as:</p> <ul style="list-style-type: none"> - Access Control - Physical and Environment Security - Supplier Security Management - Information Security - Acceptable Use - Information Classification - Operation and Communication Management - Risk Assessment Register - ISMS - Systems Acquisition Development and Maintenance - Business Continuity - Data breach response plan - Asset Management - Cryptography
<p>NYCRR - 121.9 (a)(7):</p>	<p>Describe how the organization will use encryption to protect personally identifiable information in its custody while in motion or at rest.</p>	<p>ClickView uses AES256 as our encryption standard for data in transit and rest and for backups as well.</p>
<p>NYCRR - 121.9 (a)(8):</p>	<p>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.</p>	<p>Affirm</p>

<p>NYCRR - 121.9 (a)(b):</p>	<p>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.</p>	<p>ClickView will ensure that subcontractors are only granted access to personal information to the extent needed to provide their services for us, strictly in accordance with our instructions, in accordance with applicable privacy laws, our contractual requirements, our contractual obligations to the BOCES and other customers, and not for any other commercial purpose.</p> <p>We will oversee the performance of subcontractors and ensuring that any subcontractors that ClickView will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements which are, at a minimum, materially similar and no less protective than the data protection obligations imposed on ClickView</p>
<p>NYCRR - 121.10 (a):</p>	<p>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.</p>	<p>ClickView will notify the BOCES of any privacy incident that implicates PII within 24 hours of confirmation of such incident.</p> <p>ClickView will provide in its notice to the BOCES details of the incident; how the incident has impacted PII; the steps ClickView has or will take to contain and mitigate the incident; and any proposed additional notification to regulatory bodies or data subjects.</p> <p>ClickView will cooperate with the BOCES with investigating the incident, and ClickView will consult with the BOCES and provide any further information, or take such further corrective steps, as may be deemed necessary by the BOCES to comply with any applicable law.</p> <p>ClickView will consult with the BOCES in respect of a remediation plan and the contents of any notification to impacted data subjects.</p>
<p>NYCRR - 121.10 (f):</p>	<p>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.</p>	<p>Affirm</p>
<p>NYCRR - 121.10 (f.2):</p>	<p>Please identify the name of your insurance carrier and the amount of your policy coverage.</p>	<p>Chubb Insurance:</p> <p>Professional Liability - \$2,000,000 Public and Products Liability - \$20,000,000</p>
<p>NYCRR - 121.10 (c):</p>	<p>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.</p>	<p>Affirm</p>
<p>Acceptable Use Policy Agreement:</p>	<p>Do you agree with the Capital Region BOCES Acceptable Use Policy? (Click here: http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&id=B U4QYA6B81BF)</p>	<p>I Agree</p>
<p>Privacy Policy Agreement:</p>	<p>Do you agree with the Capital Region BOCES Privacy Policy? (Click here: http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&id=B WZSQ273BA12)</p>	<p>I Agree</p>

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
Required Portal Fields Populated:	Yes
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 ClickView ("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.
Created By:	
Publish Date:	
Contact Email Address:	crbcontractsoffice@neric.org
Requesting Company:	Capital Region BOCES
Third Party Name:	ClickView
Name:	ClickView-306265