

**BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -****SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION**

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

<b>Name of Contractor</b>	<u>NCS Pearson, Inc.</u>
<b>PII Declaration</b>	<p><b>Does your organization/software collect student personally identifiable information (PII) or staff PII? – Yes: Student PII. See description below.</b></p> <p>Examples of student PII:</p> <ul style="list-style-type: none"><li>a. The student's name;</li><li>b. The name of the student's parent or other family members;</li><li>c. The address of the student or student's family;</li><li>d. A personal identifier, such as the student's social security number, student number, or biometric record;</li><li>e. Other indirect identifiers, such as the student's date of birth, place of birth, and Mother's Maiden Name;</li></ul> <p>Examples of staff APPR PII:</p> <ul style="list-style-type: none"><li>a. Teacher Id, Social Security Number, Employee Number, Biometric Record</li><li>b. Name, Mother's Maiden Name, Parent's Name</li><li>c. Birthdate, Place of Birth, Address</li><li>d. Gender, Race, Salary</li></ul> <p><input type="checkbox"/> <b>IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.</b></p>
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	Q-global collects, processes and stores the data for administering, scoring, and reporting on clinical assessments.
<b>Type of PII that Contractor will receive/access</b>	<p>Check all that apply:</p> <p><input checked="" type="checkbox"/> Student PII</p> <p><input type="checkbox"/> APPR PII</p>

<b>Contract Term</b>	Contract Start Date: 7/1/2024 Contract End Date: 6/30/2025
<b>Subcontractor Written Agreement Requirement</b>	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. (check applicable option)  <input checked="" type="radio"/> Contractor will not utilize subcontractors. <input type="radio"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> <li>             The EA can delete their data at any time using Q-global. The EA can also request in writing that Pearson delete their data. Data in dormant accounts are deleted after 2 years.           </li> </ul>
<b>Challenges to Data Accuracy</b>	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. The EA can add, update, and delete their data at any time using the application. Pearson will provide Customer and Technical Support as needed to facilitate such requests.
<b>Secure Storage and Data Security</b>	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>Q-global data are hosted at AWS US-East-1 region in Northern Virginia for US customers.</p> <p>Pearson Q-global employ many administrative, physical, and technical safeguards to protect customer data.</p> <p>Administrative safeguards include Pearson's Information Security Management Strategy based on the ISO 27001 Framework with movement towards NIST Cybersecurity Framework alignment which includes security policies and standards, information security and data privacy training for staff, least use privileges, configuration management, and formal processes for request and approval of accounts.</p> <p>Physical controls include physical lock and key, badge access systems, locking equipment cages, security guards, dedicated alarm systems, visitor logs, CCTV and video recording. For data centers, individual access is authorized only by the data center manager and based upon the individual's role, responsibilities, and</p>

business need. There is a data center control log that must be signed upon entrance and exit, and individuals must always present their access badge and display it visibly. Authorized employees must escort authorized visitors such as vendors, contractors, or consultants always in the data center.

Technical controls include firewalls, segregated virtual private clouds for products and environments, separated tiers for servers, data encryption for data at rest (AES 256) and in transit (TLS and HTTPS), role-based access and authentication, unique and complex authentication, secure coding practices, OS and application patching, and static and dynamic security scanning.


**Encryption**

Data will be encrypted while in motion and at rest.

## CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

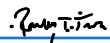
1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Contractor has implemented data security and privacy requirements in accordance with applicable federal, state, and local laws. Over the life of the Contract, Contractor will use PHI only in accordance with the Contract and applicable state, federal, and local laws. Contractor has established CISO and Privacy office with policies and standards covering all domains in security. These controls are mapped to ISO 27001, NIST, CIS.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Contractor maintains security standards appropriate to the type of data collected. Contractor has various technical and operational security controls including commercial security protection tools, security scanning tools and remediation process.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Contractor's employees, officers, and subcontractors receive training for Information Security and Data Privacy Awareness, Information Security Acceptable Use, and Code of Conduct upon hire and annually thereafter.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	<p>Prior to being hired or otherwise engaged as contractors, all Contractor personnel must submit to a criminal background check, in addition to rigorous interview- and credentials-based review.</p> <p>All employees are required to sign confidentiality agreements prior to their first day of employment.</p> <p>Where members of the workforce change positions and job responsibilities, access and permissions are adjusted accordingly.</p> <p>Upon termination, access to systems is promptly removed.</p>

5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	Contractor has various log management tools to identify security events and 24X7 Security Operations Center, Incident management team to address security incidents. Contractor will notify EA of any security event in accordance with the provisions of the Data Privacy Agreement to which this Exhibit is attached.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon expiration or termination of the Service Agreement, Contractor will transfer or destroy all data subject to the Service Agreement in accordance with the provisions of the Data Privacy Agreement to which this Exhibit is attached.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Provided as part of onboarding and customer configuration. Upon expiration or termination of the Service Agreement, Contractor will transfer or destroy all data subject to the Service Agreement in accordance with the provisions of the Data Privacy Agreement to which this Exhibit is attached.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Security policies are aligned to industry standards and best practices such as ISO 27001, NIST and CIS benchmarks
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	<p>See the embedded overview of NIST controls.</p>  <p>The image shows the cover of a document titled 'Information Security Controls' by Pearson. It includes a subtitle 'Summary of Information Security Controls: Alignment with NIST SP800-53-A' and a footer indicating it is a 'Pearson Clinical Assessment' document, dated 2024-10-4.</p>

## Western Suffolk BOCES Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at [www.nysed.gov/data-privacy-security/student-data-inventory](http://www.nysed.gov/data-privacy-security/student-data-inventory) and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to: [dpo@wsboces.org](mailto:dpo@wsboces.org). (ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-security/report-improper-disclosure](http://www.nysed.gov/data-privacy-security/report-improper-disclosure), by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to [privacy@nysed.gov](mailto:privacy@nysed.gov); or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	 <small>Randall Trask (Dec 5, 2024 06:49 MST)</small>
[Printed Name]	Randall Trask
[Title]	SVP- Clinical Assessments
Date:	12/05/2024