LIVERPOOL
CENTRAL SCHOOL DISTRICT
*Prepo,;,',-..1 our tudeKtr fo,,. ro,.,,,, rrow... Tt:ula!J*

# DATA SECURITY AND PRIVACY PLAN

**WHEREAS,** the Liverpool Central School District (hereinafter "School District") and NCS Pearson Inc (hereinafter "Contractor") entered into an agreement dated 04.05.2024 (hereinafter "Agreement") for Q-interactive (hereinafter "Services").

**WHEREAS,** pursuant to the requirements under 8 NYCRR 121, Contractor maintains the data security and privacy plan described herein in connection with the Services provided to the School District.

**1.** During the term of the Agreement, Contractor will implement all state, federal and local data security and privacy requirements, consistent with the School District's Data Security and Privacy Policy in the following way(s

**Any and all Student PII collected, processed or stored under this Agreement shall be used expressly and solely for the purposes enumerated in the agreements between the parties. The parties recognize that the use of de- identified data, which contains no personally identifiable information, is needed by Pearson in order to effectively provide, evaluate, maintain and improve its Products and Services. Providing written notice to the EA in accordance with the provisions of the Family Educational Rights and Privacy Act 20 USC 1232g and 34 CFR Part 99. In the event the EA is unable to use the functionality of the product to access or correct any requests, Pearson agrees to provide reasonable assistance to the EA.**

2. Contractor has in place the following administrative, operational and technical safeguards and practices to protect personally identifiable information that it will receive under the Agreement:

**Pearson and Q-interactive employ many administrative, physical, and technical safeguards to protect customer data.**

**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.**

**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 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..**

3. Contractor shall comply with 8 NYCRR 121 in that it acknowledges that it has reviewed the School District's Parents Bill of Rights for Data Privacy and Security and will comply with same.

a. Contractor will use the student data or teacher or principal data only for the exclusive purposes defined in the Agreement.

b. Contractor will ensure that the subcontractor(s) or other authorized persons or entities to whom Contractor will disclose the student data or teacher and principal data, if any, will abide by all applicable data protection and security requirements as described in the "Supplemental Information" appended to the Agreement.

c. At the end of the term of the Agreement, Contractor will destroy, transition or return, at the direction of the School District, all student data and all teacher and principal data in accordance with the "Supplemental Information" appended to the Agreement.

d. Student data and teacher and principal data will be stored in accordance with the "Supplemental Information" appended to the Agreement.

e. Student data and teacher and principal data in motion and at rest will be protected using an encryption method that meets the standards described in 8 NYCRR 121.

4. Prior to receiving access to student data and/or teacher and principal data, officer(s) and employee(s) of Contractor and any assignees who will have access to student data or teacher or principal data shall receive training on the federal and state laws governing confidentiality of such data. Such training shall be provided:
*Specify date of each training*

**Pearson staff members receive training for Information Security and Data Privacy Awareness, Information Security Acceptable Use, and Code of Conduct upon hire and annually thereafter.**

5. Subcontractors (select one): b. Contractor shall utilize subcontractors

a. Contractor shall not utilize subcontractors.

b. Contractor shall utilize subcontractors. Contractor shall manage the relationships and contracts with such subcontractors in the following ways in order to ensure personally identifiable information is protected:

**Subcontractors sign non-disclosure agreements. Pearson ensures that any subcontractors, or other authorized persons or entities to whom the Pearson will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements.**

6. Contractor has the following procedures, plans or protocols in place to manage data security and privacy incidents that implicate personally identifiable information: *Procedures, plans or protocols must, at a minimum, specify plans to identify breaches and unauthorized disclosures, and to promptly notify the School District.*

**Incident response processes include defined roles, workflows, and actions for responding and gathering relevant forensic information. All workforce members are provided training on their responsibility to promptly report known or suspected information security violations. The process pulls in a multi- disciplinary core team of experts to facilitate, manage, and coordinate all activities associated with the response effort. This core team is comprised of technical subject matter experts, business stakeholders, legal counsel, and information security. Other specialists are pulled in as needs of the incident dictate. The response process, though not a single-threaded process, in general flows as follows:**

- **Notification/Detection**
- **AISO Triage & Confirmation**
- **IR Core Team Formed**
- **Scope Determined**
- **Remediation**
- **Notification**
- **Post-Incident Review**

**Customers are notified within 72 hours of a confirmed security breach.**

7. Termination of Agreement.

a. Within___ days of termination of the Agreement, Contractor shall delete or destroy all student data or teacher or principal data in its possession; AND

b. D Within_____ days of termination of the Agreement, Contractor shall return all data to the School District using, OR

Transition all data to a successor contractor designated by the School District in writing

**Pearson's current data retention period is two years after a license has been inactive, we delete and obfuscate the customer data in the database. The qualified end user can submit a written request at any time to delete all business entity data. Additionally, School District can amend or delete their own data at any time using the application interface.**

8. In the event of a conflict between the terms of this Data Security and Privacy Plan and the terms of the Agreement, the terms of this Data Security and Privacy Plan shall control. All of the defined terms in the Agreement shall have the same definitions in the Data Security and Privacy Plan, unless otherwise defined herein. Except as expressly set forth in this Data Security and Privacy Plan, the terms and conditions of the Agreement shall remain unmodified and in full force and effect.

**IN WITNESS WHEREOF,** the Contractor hereto has executed this Data Security and Privacy Plan as of 04/05/2024

Randall Trask (Apr 5, 2024 10:04 MDT)

Contractor: NCS Pearson, Inc.

Title: SVP- Clinical Assessments

Date: 04/05/2024

# Parents Bill of Rights
## Liverpool Central School District

The Liverpool School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, parents and eligible students can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency.

3. State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, that protect the confidentiality of a student's PII, and 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.

4. A complete list of all student data elements collected by NYSED is available for public review and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

5. The right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints may be submitted to NYSED online, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234, by email to privacy@nysed.gov, or by telephone at 518-474-0937.

6. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

7. Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.

8. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

**APPENDIX**

*Supplemental Information Regarding Third-Party Contractors*

In the course of complying with its obligations under the law and providing educational services to District residents, the Liverpool School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following

supplemental information will be included with this Bill of Rights:

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

2. How the third-party contractor will 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 laws and regulations (e.g., FERPA; Education Law Section 2-d);

3. The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);

4. 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;

5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and

6. Address how the data will be protected using encryption while in motion and at rest.

| | |
|---|---|
| | Randall Trask (Apr 5, 2024 10:04 MDT) |
| Liverpool Administrator Signature | Representative Signature |
| | Randall Trask |
| Liverpool Administrator Printed Name | Representative Printed Name |
| | 04/05/2024 |
| Date | Date |