RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Executive Director of Technology

Vendor Statement of Compliance
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and NCS Pearson, Inc. ("Service Provider") on 11/15/2023 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

   Agree: Yes ● No ○

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

   Agree: Yes ● No ○

3. **PRIVACY**. The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Yes ● No ○

Section I: General - All Data *(Continued)*

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

   Agree: Yes ● No ○

5. **TRANSPORT**: Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

   Agree: Yes ● No ○

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

   Agree: Yes ● No ○

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

   Agree: Yes ● No ○

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

   Agree: Yes ● No ○

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Yes ● No ○

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.

   Agree: Yes ● No ○

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.

   Agree: Yes ○ No ●

   Q-interactive does not allow for student generated content.

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.

   Agree: Yes ● No ○

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

   Agree: Yes ● No ○

5. Vendor will attach to this document evidence how student data is kept secure and confidential.

   Agree: Yes ● No ○

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.

   Agree: Yes ● No ○

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).

   Agree: Yes ● No ○

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

   Agree: Yes ● No ○

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students

   Agree: Yes ● No ○

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

   Agree: Yes ● No ○

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

   Agree: Yes ● No ○

3. Vendors cannot sell student information.

   Agree: Yes ● No ○

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

   Agree: Yes ● No ○

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

   Agree: Yes ● No ○

6. Vendors must delete district-controlled student information when requested by the District.

   Agree: Yes ● No ○

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

   Agree: Yes ● No ○

As an authorized representative of my organization, I accept the conditions listed in this document.

Randall Trask
Print Name

dall Trask (Nov 16, 2023 09:50 MST) 11/16/2023
Signature, Date

Laura Assem
Print Name (Roseville City School District)

11/16/2023
Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

See attached document: Roseville City School District Additional Compliance Information

Section 1.7: Internal Security

See attached document: Roseville City School District Additional Compliance Information

Section II.2: Exporting of Student-Created Content

See attached document: Roseville City School District Additional Compliance Information

Section II.4: Review and Correcting Personally Identifiable Information (PII)

See attached document: Roseville City School District Additional Compliance Information

EXHIBITS

Section II.5: Securing Student Data

See attached document: Roseville City School District Additional Compliance Information

Section II.6: Disclosure Notification

See attached document: Roseville City School District Additional Compliance Information

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

See attached document: Roseville City School District Additional Compliance Information

Section III.5: How Student Data is Protected:

See attached document: Roseville City School District Additional Compliance Information

Organization: NCS Pearson, Inc.

Products: Q-interactive

Section I.6 External Security

Q-interactive uses AWS Shield which defends against most common, frequently occurring network and transport layer DDoS attacks that target the website or application. AWS Shield Standard is also used in conjunction with Amazon CloudFront and Amazon Route 53 which provide additional protection. These services receive comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks. AWS WAF is implemented at AWS. Q-interactive also uses VPCs with security groups controlling inbound and outbound traffic for each instance. In addition to security groups, network traffic entering and exiting each subnet is allowed or denied via network Access Control Lists.

Section I.7 Internal Security

Only a small number of Pearson database administrators have access to student data. Data are entered via a website using a standard web browser or via a native iOS iPad application.

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.

Data are backed up daily with transaction logs every 5 minutes. Data are replicated in relative real time to an alternate Availability Zone (AZ). Only a small number of Pearson database administrators have access to backup data. Backups are maintained for 7 days. Once backups the backup snapshots are deleted and not recoverable. Pearson does not print any hard copy records of student data.

Section I.8 District Access

The District can print or export their data at any time using the application in a PDF or CSV format.

Section II.2 Exporting of student-created content

Q-interactive does not allow for student generated data.

Section II.4 Review and correcting personally identifiable information

A parent, legal guardian, or student must contact the District to review or correct their PII that is collected. The District can use the application to add, update, modify, or delete any data within their account. Pearson will provide customer and technical support to facilitate such requests as needed.

Section II.5 Securing student data

All systems and data are hosted at Amazon Web Service (AWS).

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.

Section II.6 Disclosure notification

Pearson will notify the District within 72 hours in the confirmed case of an unauthorized disclosure of student records. It is the responsibility of the District to notify affected parents, legal guardians, and eligible students of the unauthorized disclosure of student records. Pearson will work with the District to provide the appropriate information to facilitate this process.

Section II.8 FERPA compliance

A parent, legal guardian, or student must contact the District to inspect, review, correct, or delete their PII that is collected. The District can use the application to add, update, modify, or delete any data within their account. Pearson will provide customer and technical support to facilitate such requests as needed.

Section III.5 How student data is protected

All systems and data are hosted at Amazon Web Service (AWS).

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.