ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

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

Laura Assem, 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 Newsela, Inc. ("Service Provider") on 5/21/2021 ("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 ○

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, Director of Technology

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 ○

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, Director of Technology

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 ○

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 ○

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

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

Laura Assem, Director of Technology

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.

Chris Mezzatesta
Print Name

DocuSigned by:
Chris Mezzatesta 5/21/2021
Signature, Date

Laura Assem, 5/22/2021
Print Name (Roseville City School District)

Signature, Date (Roseville City School District)

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, Director of Technology

EXHIBITS

Section 1.6: External Security

Newsela reduces our attack surface and maximizes uptime by not maintaining our own data centers. All user data is stored in Amazon Web Services' Relational Database Service (RDS), which is a cloud hosted version of mySQL. Data transmitted from the user to AWS is encrypted via TLS. Amazon handles encryption of the data layer itself within their data centers, along with physical security of the actual underlying hardware. Production data is within a "private cloud" behind a VPN and access is granted a limited subset of Newsela engineers via white-listed IP addresses. Monitoring and alerting systems, both native to applications and external to them, alert multiple people to security and operational issues. More information about the security of AWS is available at https://aws.amazon.com/security/.

Section 1.7: Internal Security

Access to Newsela's data is granted such that it is consistent with the principle of Least Privilege. District data is pushed to Newsela in the OneRoster format via SFTP, or via an learning platform such as Clever or Google Classroom. Data is handled by a dedicated on-boarding team. Sensitive areas of the back-end application are only accessible via VPN using a white-listed IP address. Contracted engineering personnel do not have access to production user data. Application database backups are taken nightly, encrypted, and stored on Amazon Web Services. A rotating set of backups is accessible for 30 days before being moved to cold storage on AWS Glacier. Data is not printed or maintained in a hard copy format.

Section II.2: Exporting of Student-Created Content

Student accounts in Newsela are not tied to the district's license. If Newsela's relationship with the district ends, students can still use their Newsela account to access the application. Students may transfer content to a personal account by setting their email address to a personal email address and continuing to use the service under their personal login. Individual students may transfer data by copying and pasting any content they create from their account into personal documents. Teachers or administrators using Newsela PRO may export student information by accessing the Binder and using the "Export to CSV" option.

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

Newsela does not claim ownership of user content or student data. Schools which use a learning platform such as Clever or OneRoster are responsible for correcting student data. If a student has created an account with Newsela using their name and email address, parents or legal guardians may review student's personal information by logging into the student's account, or by sending an email to support@newsela.com or postal mail to 475 10th Avenue, 4th Floor New York, NY 10019. Newsela will not respond directly to support requests from students.

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

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

Laura Assem, Director of Technology

EXHIBITS

Section II.5: Securing Student Data

Newsela has signed the Student Privacy Pledge, a rigorous, legally-enforceable commitment to student privacy developed by the Future of Privacy Forum, an industry watchdog. Our stance is outlined in our Student Privacy Pledge. More information can also be found in our Privacy Policy and Terms of Use. Newsela follows industry-standard security practices to ensure the integrity of our systems. We conduct periodic risk assessments and use commercially reasonable efforts to remediate identified security vulnerabilities. Newsela also has an incident response plan and will promptly notify the relevant School in the event of a security or privacy incident or breach of personal information involving such School's Users.

Section II.6: Disclosure Notification

Unless notification within this time limit would disrupt investigation of the incident by law enforcement, Newsela will notify the District:
(1) The security breach notification shall include, at a minimum, the following information to the extent known by Newsela and as it becomes available:
i. The name and contact information of the reporting law enforcement agency subject to this section.
ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
iii. Depending on the information available at the time the notice is provided, either
(1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(2) Newsela will adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification of affected parties and mitigation of any such data breach.
(3) Newsela will coordinate its notification activities with the District and either support the District in its notification of affected parties, or notify the affected parties directly, at the District's direction.

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

Newsela meets the requirements of FERPA. You can learn more about our FERPA compliance by visiting our Terms of Service and Privacy Policy.

Section III.5: How Student Data is Protected:

Newsela has signed the Student Privacy Pledge, a rigorous, legally-enforceable commitment to student privacy developed by the Future of Privacy Forum, an industry watchdog. Our stance is outlined in our Student Privacy Pledge. More information can also be found in our Privacy Policy and Terms of Use. Newsela follows industry-standard security practices to ensure the integrity of our systems. We conduct periodic risk assessments and use commercially reasonable efforts to remediate identified security vulnerabilities. Newsela also has an incident response plan and will promptly notify the relevant School in the event of a security or privacy incident or breach of personal information involving such School's Users.