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 Coughlan Companies, LLC dba Capstone ("Service Provider") on 03/03/2025 ("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 ●

   Vendor may access accounts to provide customer support and demonstrate product(s) functionality and entitlements. Capstone is currently reviewing this process in order to maintain compliance with all international, federal, and state data privacy laws and regulations.

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 ○

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.

Melissa Brodin
Print Name

Melissa Brodin 03/03/2025
Signature, Date

Laura Assem
Print Name (Roseville City School District)

3/13/2025
Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

To manage Capstone's IT Security and Governance program, Capstone uses the NIST Cybersecurity Framework (CSF) 2.0 and the NIST Risk Management Framework (RMF). Applications are secured with web application firewalls and segment our application service architecture using VPCs. Capstone's infrastructure is built on AWS, our cloud-hosting provider for digital products, and their recommended security pillars and standards. AWS standards ensure compliance with various security frameworks, including SOC, PCI, ISO, NIST, GDPR, and FPS, covering hardware, virtual systems, vulnerability management, patch management, internet security, and data destruction. Captone applies industry best practices to safeguard the data within our digital products. To enhance security operations, Capstone partners with a third-party security firm that provides CISO services, process reviews, penetration testing, vulnerability scanning, recommendations, and best practices. We collaborate with security partners for comprehensive security testing and assessments to support program development, risk assessments, vulnerability scans, and penetration testing. They also conduct internal, external, and web application penetration testing and provide our organization with 24/7 security monitoring, vulnerability scans, guidance on Microsoft 365 and Azure security, incident detection and containment, and monthly security improvement planning. Additionally, they assist with security assessments and the development of our security risk management program.

Section 1.7: Internal Security

Capstone has adopted and will maintain the following administrative, technical and physical safeguards, measures, and controls to manage privacy and security risks and protect the district's data in a manner that complies with all federal and state laws, rules, and regulations: (1) Only those who need it to perform their duties will have access to data; (2) Training and guidance are provided to all employees that will have access to and handling data; (3) Background checks are performed and NDAs are signed by all employees at the start of employment; (4) All access to systems and data is revoked upon employment termination; and (5) All data stored electronically is kept secure by using strong passwords, automatically enforcing employee system password updates, protecting servers with security software and firewall(s), backing up data frequently, never disclosing PII to unauthorized people within or outside of Capstone, routinely monitoring systems for security breaches and attempts of inappropriate access, and enforcing MFA and administrative controls. Engineering teams follow change control best practices, implement firewalls/web application firewalls/intrusion detection systems/intrusion prevention systems to actively inspect and block malicious traffic, follow best practice of 'least privileged permissions,' and maintain close partnership between our external security firm and cloud hosting providers. Upon written request of the district and when it is no longer needed for the purpose for which it was obtained, Capstone shall dispose of or delete all data obtained under the agreement. Disposition shall include the shredding of any hard copies of any data, data destruction, or otherwise modifying the personal information in those records to make it unreadable or indecipherable. Capstone uses multiple approaches to recover data, including redundancy, high-volume queues, daily backups, and transaction logs. We monitor our systems 24/7 for intrusions or unusual activity and have warning systems enabled. Since Capstone's products are cloud based, we follow industry standard backup and recovery processes for the data and databases in our cloud infrastructure.

Section II.2: Exporting of Student-Created Content

PebbleGo is a database of educational curriculum with informational articles, ready-made activities, and literacy supports, and does not allow for student-created content. Therefore there is no export of student-created content functionality.

As an add-on to PebbleGo, PebbleGo Create is a creation tool that allows students, educators, and administrators to create and publish original and authentic content. Student-created Projects can be downloaded and saved as a PDF, and individual slides can be downloaded and saved as a PNG. All Projects created within an account can be exported within the PebbleGo Create application to an alternative PebbleGo Create account. For a step-by-step process, please see Organizing, Copying, Importing and Deleting Projects located here:
https://www.pebblego.com/resources/help-center/using-pebblego/create-help-center

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

Parents, legal guardians, and students who seek to challenge the accuracy of PII will do so by contacting the district. If a correction to data is deemed necessary, the district will notify Capstone, and Capstone agrees to facilitate such corrections.

EXHIBITS

Section II.5: Securing Student Data

Capstone will keep student data secure and confidential by adhering to the following guidelines:

- A student's personally identifiable information cannot be sold or released for any commercial purposes
- Parents have the right to inspect and review the complete contents of their child's education record
- Capstone will follow state and federal laws which protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including, but not limited to, encryption, firewalls, and password protection will be in place when data is stored or transferred
- Capstone will limit internal access to education records to those individuals that are determined to have legitimate educational interests
- Except for authorized representatives of Capstone to the extent they are carrying out the contract or written agreement, Capstone will not disclose any personally identifiable information to any other party
- Capstone will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody
- Capstone will use encryption technology to protect data while in motion or in its custody
- Capstone will adopt technology, safeguards and practices that align with the NIST Cybersecurity Framework

Section II.6: Disclosure Notification

In the event of an unauthorized release, disclosure or acquisition of student data that compromises the security, confidentiality or integrity of the student data maintained by Capstone, Capstone shall provide notification to the district within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Capstone shall notify the district with the following:

- A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
- If the information is possible to determine at the time the notice is provided, then either the date of the breach, the estimated date of the breach, or the date range within which the breach occurred.
- 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
- A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

The district also may require that Provider provide a written notice of the breach or disclosure, as well as a description of the corrective actions taken, to any district student, parent, or employee directly impacted by the breach or disclosure. Any such notice shall be subject to review and approval by the district.

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

Capstone recognizes the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations. Under FERPA, Capstone shall be considered a School Official, under the control and direction of the district as it pertains to the use of student data. Throughout the life of the contract, Capstone will:

- Limit internal access to education records to those individuals that are determined to have legitimate educational interests
- Not use the education records for any other purposes than those explicitly authorized in its contract or written agreement. Unauthorized use includes selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to another third-party for marketing or commercial purposes except for authorized representatives of Capstone to the extent they are carrying out the contract or written agreement.
- Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of protected information in its custody
- Agree that all student data transmitted to Capstone is and will continue to be the property of and under the control of the district
- Require that officers and all employees of Capstone who have access to student, teacher or principal data receive ongoing training surrounding the federal and state laws governing confidentiality of the data.
- Request that parents, teachers, or principals who seek to challenge the accuracy or deletion of protected information will do so by contacting the district. If correction or deletion of data is deemed necessary, the district will notify Capstone in writing, and Capstone agrees to facilitate such requests.
- Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using modern technologies or methodologies
- Adopt technology, safeguards, and practices that align with the NIST Cybersecurity Framework
- Impose all the terms stated above in writing where Capstone engages a subcontractor or other party to perform any of its contractual obligations, which provide access to protected information.

Section III.5: How Student Data is Protected:

Student information is protected through Capstone's use of industry best practices. Our PebbleGo suite (PebbleGo, PebbleGo Next, and PebbleGo Spanish) as well as Capstone Interactive eBooks do not utilize individual student accounts. Instead, these products operate with a single shared building account for all students and educators. These products do not collect personally identifiable student information such as usernames, passwords, names, or student-generated content. PebbleGo Create is a creation tool that does utilize individual student accounts and therefore contains student information. To access PebbleGo Create, Capstone employs a range of secure login methods, including Username/Password (U/P), Okta Single Sign-on (SSO), Multifactor Authentication (MFA) through Clever or ClassLink, and Saved Password Systems. Capstone utilizes the NIST Cybersecurity framework in combination with the CIS Controls, NIST 800-53, and other relevant control frameworks to manage our security program. We work with third party security firms to perform at minimum annual risk assessments, penetration tests, and vulnerability scans of our customer-facing and internal IT systems.