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 Vista Higher Learning, Inc. ("Service Provider") on 09/13/2023 ("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 "Data" or "data" as used below means "Pupil Records" as defined in AB 1584.

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. Vendor may copy or duplicate data only as necessary to provide the contracted Services.

   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. LEA will provide written request to vendor first to delete data and allow 60 days for deletion.

   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. Except as needed to provide the Services and engaged by Contractor to provide services to all customers of Contrac
(such as Amazon Web Services, Inc. (AWS), which provides infrastructure-as-a-service to host Digital Components
provided under this Agreement, and Altavista Solutions and ONELINK S.A.S NIT, each of which provides outsourced he
desk agents in support of Contractor’s 24x7 customer support services for digital components).

   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). Data will be deleted upon written request of the district.

   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. And as allowable by law.

   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. Requests will be ma
   in writing.

   Agree: Yes ● No ○

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

   Agree: Yes ● No ○

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

Jon Aram, CEO of Vista Higher Learning, Inc.	Laura Assem
Print Name	Print Name (Roseville City School District)
Jon Aram Digitally signed by Jon Aram Date: 2023.09.13 16:36:24 -04'00'	10/2/2023
Signature, Date	Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

SOC 2 Type 2 Security audit report will be provided upon execution of a Mutual NDA. Note that all data and applications are operated through Amazon Web Services (AWS) cloud hosting centers in the US. Applications are tested annually by third party security services, and specifically Rapid 7.

Section 1.7: Internal Security

SOC 2 Type 2 Security audit report will be provided upon execution of a Mutual NDA.

Section II.2: Exporting of Student-Created Content

If Student-Generated Content is stored or maintained by the Vendor as part of the Services,Vendor shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student• Generated Content to a separate account created by the student upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.

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

To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Vendor shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Vendor to view or correct as necessary. In the event that a parent of a student or other individual contacts the Vendor to review any of the Student Data accessed pursuant to the Services, the Vendor shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

EXHIBITS

Section II.5: Securing Student Data

SOC 2 Type 2 Security audit report will be provided upon execution of a Mutual NDA. Note that data is encrypted in transit using TLS 1.2 and at rest using AES 256.

Section II.6: Disclosure Notification

In the event of an unauthorized release, disclosure or acquisition of Data that compromises the security, confidentiality or integrity of the Data maintained by the Vendor the Vendor shall provide notification to LEA 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.

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

For the purposes of FERPA, the Vendor shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Data.

Section III.5: How Student Data is Protected:

SOC 2 Type 2 Security audit report will be provided upon execution of a Mutual NDA.

Reset Form