

**CALIFORNIA STUDENT DATA PRIVACY  
AGREEMENT Version 2.0 (September 26, 2018)**

**School District/Local Education Agency:**

**Campbell Union High School District**

**AND**

**Provider:**

**Aeries Software, Inc. DBA Eagle Software**

**Date:**

**11/13/2019**

2. **Nature of Services Provided.** The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit “A” hereto:
3. **Student Data to Be Provided.** The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit “B”.
4. **DPA Definitions.** The definition of terms used in this DPA is found in Exhibit “C”. In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

## ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil’s records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA’s request for Student Data in a pupil’s records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** If pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit “A”, Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.
4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party.

attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data**. Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a “Request for Return or Deletion of Student Data” form, a copy of which is attached hereto as Exhibit “D”. Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may request partial disposal of Student Data obtained under the Service Agreement that is no longer needed. Partial disposal of data shall be subject to LEA’s request to transfer data to a separate account, pursuant to Article II, section 3, above.

b. **Complete Disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement Provider shall dispose or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3, above. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

6. **Advertising Prohibition**. Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

## ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of

monitoring and assessments of Subprocessors to determine their compliance with this Article.

- h. Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

**2. Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. Provider shall follow the following process:

- a.** The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described herein under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.
- b.** The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
  - i.** The name and contact information of the reporting LEA 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.** If the information is possible to determine at the time the notice is provided, then 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.
  - v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- c.** At LEA’s discretion, the security breach notification may also include any of the following:
  - i.** Information about what the agency has done to protect individuals whose information has been breached.
  - ii.** Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d.** Provider agrees to adhere to all requirements in applicable State and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before:

**a. Designated Representatives**

The designated representative for the LEA for this Agreement is:

Name: Nancy Torres Pfeiffer  
Title: Assistant Superintendent of Business

Contact Information:  
npfeiffer@cuhsd.org  
\_\_\_\_\_  
\_\_\_\_\_

The designated representative for the Provider for this Agreement is:

Name: Brent Lloyd  
Title: Vice President

Contact Information:  
brent@aeries.com  
(888)-487-7555  
\_\_\_\_\_  
\_\_\_\_\_

**b. Notification of Acceptance of General Offer of Terms.** Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, to the designated representative below.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: Brent Lloyd  
Title: Vice President

Contact Information:  
brent@aeries.com  
(888)-487-7555  
\_\_\_\_\_  
\_\_\_\_\_

**6. Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and


**IN WITNESS WHEREOF**, the parties have executed this California Student Data Privacy Agreement as of the last day noted below.

Provider: **Aeries Software, Inc. DBA Eagle Software**

BY:  Date: 11/13/19

Printed Name: **Brent Lloyd** Title/Position: **Vice President**

Local Education Agency: **Campbell Union High School District**

BY:  Date: 11/13/2019

Printed Name: Nancy Torres Pfeiffer Title/Position: Assistant Superintendent of Business

***Note: Electronic signature not permitted.***

**EXHIBIT "B"**

**SCHEDULE OF DATA**

<b>Category of Data</b>	<b>Elements</b>	<b>Check if used by your system</b>
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	X
	Other application technology meta data-Please specify:	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	<b>X</b>
	Observation data	<b>X</b>
	Other assessment data-Please specify:	x
Attendance	Student school (daily) attendance data	x
	Student class attendance data	x
Communications	Online communications that are captured (emails, blog entries)	x

Conduct	Conduct or behavioral data	x
Demographics	Date of Birth	x
	Place of Birth	x
	Gender	x
	Ethnicity or race	<b>X</b>
	Language information (native, preferred or primary language spoken by student)	x
Enrollment	Other demographic information-Please specify:	x
	Student school enrollment	<b>X</b>
	Student grade level	<b>X</b>
	Homeroom	x
	Guidance counselor	<b>X</b>
	Specific curriculum programs	x
	Year of graduation	<b>X</b>
Other enrollment information-Please specify:	x	
Parent/Guardian Contact Information	Address	x
	Email	x
	Phone	x

	work data - Please specify:	X
Transcript	Student course grades	X
	Student course data	X
	Student course grades/perfor- mance scores	X
	Other transcript data -Please specify:	X
Transportation	Student bus assignment	X
	Student pick up and/or drop off location	X
	Student bus card ID number	X

	Other transportation data -Please specify:	X
Other	Please list each additional data element used, stored or collected by your application	X

No Student Data Collected at this time \_\_\_\_\_.  
\*Provider shall immediately notify LEA if this  
designation is no longer applicable.

OTHER: Use this box, if more space needed.



**Pupil Records:** Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

**Service Agreement:** Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

**School Official:** For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

**SOPIPA:** Once passed, the requirements of SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

**Student Data:** Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and federal laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

**SDPC (The Student Data Privacy Consortium):** Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

**EXHIBIT "D"**

**DIRECTIVE FOR DISPOSITION OF DATA**

Campbell Union High School District directs Aeries Software, Inc. DBA Eagle S<sub>3</sub> to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

<p><b><u>Extent of Disposition</u></b></p> <p>Disposition shall be:</p>	<p><u>        </u> Partial. The categories of data to be disposed of are as follows:</p> <p><input checked="" type="checkbox"/> Complete. Disposition extends to all categories of data.</p>
<p><b><u>Nature of Disposition</u></b></p> <p>Disposition shall be by:</p>	<p><u>        </u> Destruction or deletion of data.</p> <p><input checked="" type="checkbox"/> Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data.</p>
<p><b><u>Timing of Disposition</u></b></p> <p>Data shall be disposed of by the following date:</p>	<p><input checked="" type="checkbox"/> As soon as commercially practicable</p> <p><u>        </u> By (Insert Date) _____</p>

**John Keating**

\_\_\_\_\_  
Authorized Representative of LEA

11/13/2019

\_\_\_\_\_  
Date

**Brent Lloyd**

\_\_\_\_\_  
Verification of Disposition of Data  
by Authorized Representative of Provider

11/13/2019

\_\_\_\_\_  
Date

## **EXHIBIT “F” DATA SECURITY REQUIREMENTS**

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]

Aeries hosted clients' data resides in a data center that is SOC 2., SOC 3, HIPAA & PCI compliant with stringent security, top-tier fire suppression and 2.4x7 site monitoring. The facility also has key card, biometric, mantrap, alarm, and video surveillance systems. The site is manned 2.4/7.

All hardware is behind extensive hardware firewalls. The web servers use SSL for all network traffic to and from the servers. Any direct connections to the hosted Microsoft SQL databases are encrypted. Additionally, the external IP address of the client computer accessing the database directly must be added in our firewall to receive access. Any direct access to the web or database servers requires Microsoft Azure multi-factor authentication.