AN OVERVIEW OF THE CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

Introduction: Since the passage of AB 1584, (now found at California Education Code section 49073.1), school districts have struggled to incorporate its required provisions in their contracts with digital providers. Two reasons account for a large portion of these difficulties. First, school districts often do not have the legal resources to negotiate with legally compliant privacy provisions, especially when they are negotiating with digital providers who may be resistant to change contract provisions the providers have crafted for their own purposes often at considerable expense. Second, other school districts are often reluctant to adopt the products for their school district, especially if they do not know whether these other agreements have been legally reviewed, and by persons who are comfortable in the new law of data privacy.

The California Student Data Privacy Agreement (referred to here as the "DPA") attempts to tackle these two challenges head on. First, it has been reviewed by several sets of legal and subject matter experts ranging from the Federal government, private attorneys, and educators working in the data privacy field both within the State of California and beyond. Users of this document can know, with a high degree of confidence, that it meets both the requirements of Federal and California State law.

School districts using this DPA for their digital contracts can, by uploading the executed DPA into the California Student Privacy Alliance ("CSPA") website, make the DPA available for use by other school districts. This includes school districts both within California and outside of California, since California is now a member of a nationwide data contract exchange maintained by the Student Data Privacy Consortium ("SDPC").

Practical Document: Legal compliance was not the only objective of the drafters of this DPA. They also sought to make this a practical and useful document; therefore this document contains provisions that will be of assistance to those persons, at the District and the Vendors who will administer the digital program established by the underlying agreement. We will briefly note some of the more important provisions of the DPA:

(a) *Nature of Digital Services*: Paragraph 2 of Article I of the DPA describes the service to be provided by the digital vendor. Such a description is often missing in many digital contracts. Having a short and workable summary of the services will also provide a description of the benefits of such a service to members of the educational community, a vital component in the acceptance and dissemination of educational digital products.

(b) *Types of Data to be Transferred*: Paragraph 3 of Article I, provides an opportunity for the Vendor and the District to list the types of student data that the providers will need in order to perform its services. This listing can be accomplished either by listing the types of data to be transferred in the text of the DPA or by checking the data "boxes" in Exhibit B, the Schedule of Data, attached to the DPA.

(c) *Descriptions of Data Security*. This provision is found at Paragraph 1 of Article V. It was perhaps the most challenging section of the DPA, especially given the lack of specific data security requirements in California law. We therefore resorted to some helpful categories of data protection, (including regulating Provider Subprocessors, a topic often neglected in the law). The paragraph while also allowing the provider to flesh out their security measures in an attachment to the DPA. We are optimistic that provider attachments will increase public confidence in digital products, because it has been our experience that many digital providers have elaborate and robust data security systems.

(d) *Definitions:* In development of the DPA, we found that different laws used identical terms but with different meanings. To avoid confusion and enable all stakeholders to understand the DPA, we felt an important component was a Definition of Terms or Exhibit C.

Partnership: Readers of this DPA may detect a more "neutral" tone than that found in many DPAs and which takes into account provider interests. This includes the creation of commensurate data protection duties for school districts. This approach is deliberate. The authors of this DPA believe that to be effective, digital contracts must create a partnership, a recognition that is as vitally important to providers as well as school district to protect the integrity of student data.

Scalability: Perhaps the most ambitious section of the DPA is the "General Offer of Terms" by the Provider regarding student data privacy rights. Providers making this voluntary offer (found at Exhibit "E"), agree to be bound to the same privacy terms as found in the DPA to other, future school districts who also sign the DPA. Why would a provider ascribe to this offer? Because they, like school districts, also wish to avoid the transaction costs and uncertainties of separately negotiating the privacy sections of their data agreements with individual school districts. They are also protected by the fact that the privacy offer does not include such items as pricing, which the providers are free to negotiate separately, and by the limited duration of the offer.

Length: The drafting of contracts frequently involves the sacrifice of certain principles. Here the sacrificed quality may be compactness. This DPA is rather long, but it is long for four reasons. First, it hopes to be versatile and used in a number of settings. To do so it must be comprehensive. Secondly in order to be useful, it employs several attachments which could, in the appropriate circumstances, be discarded. Third, the formatting and font size is generous for ease of reading. The font size can be decreased. Finally, the world of digital education is complicated and changing. Perhaps it is in this is the one context where we can venture to say that brevity is not a virtue.

Mechanics: Here are a few practical tips to help you complete the DPA:

The DPA is provided in .pdf format with fillable fields. To see the text that needs to be replaced, hover over the fillable fields. On a MAC, to see the text that needs to added,
you may need to hover on the fillable field and select Control.

On the specified pages, you will need to:

On Cover Page:

Locate fillable field **Insert Name Of School District or Local Education Agency** and insert the name of your LEA.
Locate fillable field **Insert Name of Provider** and insert the name of the Provider.
Locate fillable field **Date of Service Agreement** and insert the actual date of the agreement.

On Page 1:

Locate fillable field Insert **Name Of School District or Local Education Agency** and insert the name of your LEA.
Locate fillable field **Insert Name of Provider** and insert the name of the Provider.
Locate fillable field **Insert Date** and insert the date of the agreement.
Locate second fillable field **Insert Date** and insert the date of the agreement.

On Page 2:

Locate fillable field **Insert Brief Description of Services** and insert See Exhibit A or mark Not Applicable.

On Page 3:

Locate fillable field **Insert Categories of Student Data to be provided to the Provider** and insert See Exhibit B or mark Not Applicable.

On Page 8:

Locate fillable field **Insert County** and insert the name of the jurisdictional county.

On Page 9:

Locate fillable field **Insert Name of School District or LEA** and insert the name of the LEA.
Locate fillable field **Signature No Electronic Signatures Allowed** and manually sign the CDSPA.
Locate fillable field **Date of Service Agreement** and insert the date signed by the LEA.
Locate fillable field **Printed Name** and insert the name of the individual signing on behalf of the LEA.
Locate fillable field **Title/Position** and insert the title/position of the individual signing on behalf of the LEA.
Locate second fillable field **Insert Name of Provider** and insert the name of the Provider.
Locate second fillable field **Signature No Electronic Signatures Allowed** and manually sign the CDSPA.
Locate second fillable field **Date of Service Agreement** and insert the date signed by the Provider.
Locate second fillable field **Printed Name** and insert the name of the individual signing on behalf of the Provider.
Locate second fillable field **Title/Position** and insert the title/position of the individual signing on behalf of the Provider.

On Page 10:

Locate fillable field **Insert Detailed Description of Services Here** found as Exhibit A and insert Description of Services or mark Not Applicable.

On Pages 11-12:

Locate fillable fields **Check If Use By Your System** and check appropriate data element boxes.

On Page 16:

Locate fillable field **Insert Additional Data Security Requirements Here** found as Exhibit D and insert Data Security Requirements or mark Not Applicable.

For Providers who wish to sign the General Offer of Terms:

On Page 17 #1 Offer of Terms:

Locate fillable field **Insert Name of Initiating LEA** and insert the name of the initiating LEA.
Locate fillable field **Insert Date** and insert the date of the original initiating DPA.
Locate fillable field **Insert Provider Name** and insert the name of the Provider.
Locate fillable field **Signature No Electronic Signatures Allowed** and manually sign the General Offer of Terms.
Locate fillable field **Date** and insert the date signed by the Provider.
Locate fillable field **Printed Name** and insert the name of the individual signing on behalf of the Provider.
Locate fillable field **Title/Position** and insert the title/position of the individual signing on behalf of the Provider.

For Subscribing LEAs who wish to accept the General Offer of Terms signed by a given Provider:

On Page 17 #2 Subscribing LEA (without making any changes to #1)

Locate fillable field **Insert Subscribing LEA Name** and insert the name of the LEA.
Locate fillable field **Signature No Electronic Signatures Allowed** and manually sign the General Offer of Terms.
Locate fillable field **Date** and insert the date the Subscribing LEA accepts the General Offer of Terms.
Locate fillable field **Printed Name** and insert the name of the individual signing on behalf of the Subscribing LEA.
Locate fillable field **Title/Position** and insert the title/position of the individual signing on behalf of the Subscribing LEA.

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

Version 1.0

Capistrano Unified School District

and

Aeries Software, Inc. DBA Eagle Software

12/01/2017

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Capistrano Unified School District (hereinafter referred to as "LEA") and Aeries Software, Inc. DBA Eagle S (hereinafter referred to as "Provider") on 12/01/2017. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated 07/01/2017 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive and the LEA may provide documents or data that are covered by several federal and statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232 h; and

WHEREAS, the documents and data transferred from California LEAs are also subject to several California student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act (sometimes referred to as either "SB 1177" or "SOPIPA") found at California Business and Professions Code section 22584; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms", agrees to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable privacy statutes, including the FERPA, PPRA, COPPA, SB 1177 (SOPIPA), and AB 1584. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.

2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational services described below and as may be further outlined in Exhibit "A" hereto:

3. **Student Data to Be Provided**. In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Exhibit "B":

See Attachment for 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 or any other Pupil Records 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 Parties agree that as between them all rights, including all intellectual property rights in and to Student Data or any other Pupil Records 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 personally identifiable information on 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 reasonably timely manner to the LEA's request for personally identifiable information 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 Pupil Records of 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**. Provider shall, at the request of the LEA, transfer Student generated content to a separate student account.

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 unless legally prohibited.

5. **No Unauthorized Use**. Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in the Service Agreement.

6. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree protect Student Data in manner consistent with the terms of this DPA

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With FERPA**. LEA shall provide data for the purposes of the Service Agreement in compliance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. section 1232 g, AB 1584 and the other privacy statutes quoted in this DPA.

2. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

3. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

4. **District Representative**. At request of Provider, LEA shall designate an employee or agent of the District as the District representative for the coordination and fulfillment of the duties of this DPA.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all California and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, AB 1584, and SOPIPA.

2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of FERPA laws with respect to the data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure**. Provider shall not disclose any data obtained under the Service Agreement in a manner that could identify an individual student to any other entity in published results of studies as authorized by the Service Agreement. Deidentified information may be used by the vendor for the purposes of development and improvement of educational sites, services, or applications.

5. **Disposition of Data**. Provider shall dispose of all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within 60 days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the 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. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

6. **Advertising Prohibition**. Provider is prohibited from using Student Data to conduct or assist targeted advertising directed at students or their families/guardians. This prohibition includes the development of a profile of a student, or their families/guardians or group, for any commercial purpose other than providing the service to client. This shall not prohibit Providers from using data to make product or service recommendations to LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in in Exhibit "D" hereto. These measures shall include, but are not limited to:

    a. **Passwords and Employee Access**. Provider shall make best efforts practices to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. As stated elsewhere in this DPA, employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.

    b. **Destruction of Data**. Provider shall destroy all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was

obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.

d. **Employee Training**. The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

e. **Security Technology**. When the service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology protects information, using both server authentication and data encryption to help ensure that data are safe secure only to authorized users. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.

f. **Security Coordinator**. Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement

g. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

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. 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. Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. Provider shall assist LEA in these efforts.

e. At the request and with the assistance of the District, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms ("General Offer"), (attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the Acceptance on said Exhibit. The Form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall

destroy all of LEA's data pursuant to Article V, section 1(b).

4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and AB 1584. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the addresses set forth herein.

6. **Application of Agreement to Other Agencies**. Provider may agree by signing the General Offer of Privacy Terms be bound by the terms of this DPA for the services described therein for any Successor Agency who signs a Joinder to this DPA.

7. **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 either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

8. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

9. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF CALIFORNIA,

WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS LOCATED IN Orange COUNTY, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

[*Signature Page Follows*]

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

Capistrano Unified School District

Date: 12/01/2017

Printed Name: Jeremy Davis Title/Position: CTO

Aeries Software, Inc. DBA Eagle Software

Date: 12/01/2017

Printed Name: Brent Lloyd Title/Position: Vice President

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

Aeries is a student information system that was established in 1995. Since opening, Aeries Software has successfully implemented the Aeries Student Information System in over 600 school districts and education agencies, becoming the state's most popular SIS software. Aeries offers a software as a service solution which includes hosting and maintaining over 250 California school districts' databases.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	✓
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	✓
Assessment	Standardized test scores	✓
	Observation data	✓
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	✓
	Student class attendance data	✓
Communications	Online communications that are captured (emails, blog entries)	✓
Conduct	Conduct or behavioral data	✓
Demographics	Date of Birth	✓
	Place of Birth	✓
	Gender	✓
	Ethnicity or race	✓
	Language information (native, preferred or primary language spoken by student)	✓
	Other demographic information-Please specify:	✓
Enrollment	Student school enrollment	✓
	Student grade level	✓
	Homeroom	✓
	Guidance counselor	✓
	Specific curriculum programs	✓
	Year of graduation	✓
	Other enrollment information-Please specify:	✓
Parent/Guardian Contact Information	Address	✓
	Email	✓
	Phone	✓
Parent/Guardian ID	Parent ID number (created to link parents to students)	✓
Parent/Guardian Name	First and/or Last	✓

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	✓
	Teacher names	✓
Special Indicator	English language learner information	✓
	Low income status	✓
	Medical alerts	✓
	Student disability information	✓
	Specialized education services (IEP or 504)	✓
	Living situations (homeless/foster care)	✓
	Other indicator information-Please specify:	✓
Category of Data	**Elements**	**Check if used by your system**
Student Contact Information	Address	✓
	Email	✓
	Phone	✓
Student Identifiers	Local (School district) ID number	✓
	State ID number	✓
	Vendor/App assigned student ID number	✓
	Student app username	✓
	Student app passwords	✓
Student Name	First and/or Last	✓
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	✓
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	✓
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	✓

Category of Data	Elements	Check if used by your system
Other	Other student work data - Please specify:	✓
Transcript	Student course grades	✓
	Student course data	✓
	Student course grades/performance scores	✓
	Other transcript data -Please specify:	✓

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	✓

EXHIBIT "C"

DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code § 49073.1, relating to pupil records.

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Operator: For the purposes of SB 1177, SOPIPA, the term "operator" means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in AB 1584.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes, without limitation, at least the following:

First and Last Name	Home Address
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the Service Agreement the term "Provider" replaces the term "Third Party as defined in California Education Code § 49073.1 (AB 1584, Buchanan), and replaces the term as "Operator" as defined in SB 1177, SOPIPA.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

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 local educational LEA employee.

SB 1177, SOPIPA: Once passed, the requirements of SB 1177, SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

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 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 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

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.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection,

analytics, storage, or other service to operate and/or improve its software, and who has access to PII. This term shall also include in it meaning the term "Service Provider," as it is found in SOPIPA.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" as appears in California Education Code § 49073.1 (AB 1584, Buchanan) means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DATA SECURITY REQUIREMENTS

See attachment for Exhibit D.

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Capistrano Unified Scho and which is dated 12/01/2017 to any other LEA ("Subscribing LEA") to anywho accepts this General Offer though its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the California Student Privacy Alliance in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

Aeries Software, Inc. DBA Eagle Software

Date: 12/01/2017

Printed Name: Brent Lloyd

Title/Position: Vice President

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

Date:

Printed Name:

Title/Position

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

AERIES SOFTWARE

EXHIBIT D – DATA SECURITY REQUIREMENTS

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 24x7 site monitoring. The facility also has key card, biometric, mantrap, alarm, and video surveillance systems. The site is manned 24/7.

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.

Aeries SIS requires strong password usage through the system. Aeries SIS requires the following:

-The password may not be the same as the username.

-The password may not be "admin".

-Aeries has compiled a list of commonly used passwords using data published by outside sources. If the user attempts to use a password on this list, they will get a warning message: "Please select a more unique password."

Additionally, the LEA can set more stringent password requirements and expirations including:

-Force users to Change Passwords Every... – How often the users need to change their password.

-Days Prior to Expiration to Notify Users - Used to give the users a warning message that their password will expire several days prior to the expiration.

-Minimum Length - Defines the minimum character length of the password.

-Require Special Character - Requires that at least one non-alpha numeric character is used in the password. For example, * & % $ # @

-Require Letters and Numbers - Requires that at least one letter and one number are used in the password.

-Require Upper and Lower Case - Requires that both upper and lower-case letters are used in the password.

-New must be significantly different than old - Requires that the new password be significantly different than the existing password

Aeries includes a Records Transfer feature that can transfer supplemental data between LEAs. The Records Transfer feature was developed with an emphasis on security. Below are highlights of the security built in to the Records Transfer feature:

All data is transmitted securely via HTTPS, specifically the more secure TLS 1.2 protocol.

The student data is transmitted point-to-point between districts using private Aeries APIs and never stored on any intermediate server.

Aeries uses a centralized registry of unique district authorization codes and district Aeries URLs to validate records requests. This prevents an unknown party from forging a records request under the guise of a legitimate Aeries district.

Records Transfer uses public key encryption to encrypt all student-related data end-to-end. The data can only be decrypted using the private key of the correct receiving district.