



iKeepSafe Product Profile *Aeries Software, Inc.*

Introduction

The iKeepSafe Privacy Program is available to operators and service providers of websites and online services, data management systems and other technologies that are, in whole or in part, intended for use in and by schools, and which may collect, store, process or otherwise handle student data.

This *iKeepProfile* is intended to assist you in determining whether the Aeries Software, Inc. complies with FERPA, SOPIPA and CSPC. It indicates that Aeries Software, Inc. has been assessed for alignment with the iKeepSafe Program Guidelines.

Product Overview

Aeries Software:

Aeries is a Student Information System that serves around 650 California school districts. Aeries interfaces with district administrators, teachers, parents, and students. The student information system holds all data related to state reporting requirements as well as advanced features focused on student success. Aeries also partners with two other vendors to provide Aeries Communications and Aeries Financials.

<http://www.aeries.com/>

Agreement

As related to the Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. Section 1232g), Aeries Software, Inc. agrees:

1. Student records obtained by Aeries Software, Inc. from an educational institution continue to be the property of and under the control of the educational institution. The educational institution retains full ownership rights to the personal information and education records it provides to Aeries Software, Inc..
2. Aeries Software, Inc. users may retain possession and control of their own generated content.
3. Aeries Software, Inc. will not use any information in a student record for any purpose other than those required or specifically permitted by the Aeries Software, Inc. Terms and Conditions and Privacy Policy.
4. Parents, legal guardians, or eligible students may review personally identifiable information in the student's records and correct erroneous information by contacting their educational institution. Additionally, Aeries Software, Inc. users may access, correct, update, or delete personal information in their profile by signing into Aeries Software, Inc., accessing their Aeries Software, Inc. account, and making the appropriate changes.
5. Aeries Software, Inc. is committed to maintaining the security and confidentiality of student records. Towards this end, we take the following actions:
 - a. we limit employee access to student data to only those employees with a need to such access to fulfill their job responsibilities;
 - b. we conduct background checks on our employees that may have access to student data;
 - c. we conduct regular employee privacy and data security training and education; and
 - d. we protect personal information with technical, contractual, administrative, and physical security safeguards in order to protect against unauthorized access, release or use.
6. In the event of an unauthorized disclosure of a student's records, Aeries Software, Inc. will promptly notify users unless specifically directed not to provide such notification by law enforcement officials.
7. Aeries Software, Inc. will delete or de-identify personal information when it is no longer needed, upon expiration or termination of our agreement with an educational institution with any deletion or de-identification to be completed according to the terms of our agreement with the educational institution, or at the direction or request of the educational institution.
8. Aeries Software, Inc. agrees to work with educational institution to ensure compliance with FERPA and the Parties will ensure compliance by providing parents, legal guardians or eligible students with the ability to inspect and review student records and to correct any inaccuracies therein as described above.
9. Aeries Software, Inc. prohibits using personally identifiable information in student records to engage in targeted advertising.
10. Aeries Software, Inc. will not make material changes to our Terms of Use or Privacy Policy, including making significant changes impacting the collection, use, disclosure or retention of data collected without prior notice to the educational user.

As related to the Student Online Personal Information Protection Act (SB 1177 -“SOPIPA”), Aeries Software, Inc. agrees:

1. Aeries Software, Inc. does not target advertising via the Aeries Software, Inc. service or on any other website using information about a K-12 student, their families/guardians or educators acquired from a use of the technology.
2. Aeries Software, Inc. does not use information, including persistent unique identifiers, created or gathered by the Aeries Software, Inc. service to amass a profile about a K–12 student, their families/guardians or educators except in furtherance of K–12 school purposes.
3. Aeries Software, Inc. does not and will not sell, rent, or otherwise provide personally identifiable information to any third party for monetary gain.
4. Aeries Software, Inc. does not disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

Data Review Process

Aeries Software, Inc. provides users direct access to the personally identifiable information that they provide to Aeries Software, Inc. via product functionality. Users also have the ability to contact Aeries Software, Inc. for access to all personal information on file by contacting Aeries Software, Inc. through legal@aeries.com.

We have added to the Aeries Privacy Policy:

Your Educational Institution determines the information collected, maintained, and processed using Aeries’ services. Your Educational Institution retains the right to review, modify, and/or refuse to permit further collection or use of student data information at any time. Your Educational Institution uses Aeries’ services to assist with the administration of school-related activities and to provide a streamlined way to collect, organize, access, and report your information for educational purposes. These uses are specific to each Educational Institution and are governed by the contract between Aeries and your Educational Institution. If you have any questions regarding the collection, storage, and use of the information your Educational Institution shares with Aeries, please contact your Educational Institution directly.

General inquiries related to privacy may be directed to:

Aeries Software, Inc.

James Mallory
Vice President of Operations
770 The City Drive South, Suite 6500
Orange, CA 92868
888-487-7555
Legal@aeries.com.

Security Protocols

Aeries Software, Inc. has a comprehensive Security Program in place designed to protect the confidentiality, integrity and availability of systems, networks and data. The following is a general overview of data security protocols:

Data in Transit

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

Data at Rest

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.

Data Center Security

Aeries Software, Inc. uses AWS and these data centers conform to the following:

Aeries hosted clients' data resides in a data center that is SOC 2 certified 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.

<https://aws.amazon.com/compliance/data-center/controls/>
<https://aws.amazon.com/compliance/>

Personnel

Background Checks: All employees with access to student data have undergone criminal background checks.

Training: Employees of Aeries Software, Inc. will receive annual privacy and security training that includes FERPA.

Access: Access to student data is role-based; limited to those employees who need access to perform job responsibilities.

Employees are given access to the minimum services that are required for their job function.

Access to Audit

Once per year, Aeries Software, Inc. will provide schools with:

- audit rights to the school's data
- access to the results of Aeries Software, Inc.' or its third-party security audit

Data Breach

In the event of an unauthorized disclosure of a student's records, Aeries Software, Inc. will promptly notify users unless specifically directed not to provide such notification by law enforcement officials. Notification shall identify:

- a. the date and nature of the unauthorized use or disclosure;
- b. the Private Data used or disclosed;
- c. general description of what occurred including who made the unauthorized use or received the unauthorized disclosure;
- d. what Aeries Software, Inc. has done or shall do to mitigate any effect of the unauthorized use or disclosure;
- e. advice to the impacted user on how they can best protect themselves.
- f. what corrective action Aeries Software, Inc. has taken or shall take to prevent future similar unauthorized use or disclosure; and
- g. who at Aeries Software, Inc. the user can contact. Aeries Software, Inc. will keep the user fully informed until the incident is resolved.

Aeries Software, Inc. will notify impacted user (s) within 72 hours upon the discovery of a breach of security that results in the unauthorized release, disclosure or acquisition of student information,

Data Deletion

Aeries states they will retain your information for as long as your account is active, or as needed to provide you with our services. Please contact us at the email address at legal@aeries.com. should you wish to cancel your account or request that we no longer use your information to provide you services. We will retain and use your information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

Research

Aeries Software, Inc. stated; We use none of the customer data for research or statistical purposes at this time. If we use any customer database for troubleshooting or conducting research, the data is de-identified and no Student PII is available to view.

Aeries engineers developed an obfuscation script to remove personally identifiable information and email addresses that gets run on any incoming database from our districts.

Third Parties

Aeries Software, Inc. does not sell, trade, lease or loan the personal information they collect or maintain, in the course of providing the service, to any third party for any reason, including direct marketers, advertisers, or data brokers.

Aeries Software, Inc. contracts with other third-party companies to perform business functions or services on their behalf and may share PII with such third parties as required to perform their functions. Aeries Software, Inc. has agreements in place with all third parties with access to student personal information to ensure they only use the information for purposes necessary to deliver the authorized service and to ensure they maintain the confidentiality and security of the information. The agreements align with Aeries Software, Inc.' data privacy and security policies and expectations.

Aeries Software, Inc. utilizes the following third-party vendors:

- ApexSQL
- Attendance Works
- Canvas
- CareDox
- Catapult EMS
- CBS Complete Business Systems
- Certica
- Clever
- CPSI
- Decision Insite
- DUO
- eBackpack
- Gauge
- GoWrite
- Hayes Software Systems
- Illuminate Ed.
- Kimono
- Level Data
- Meet the Teacher
- Microsoft Learning
- Principals Exchange
- PTM document systems
- SafeSchools
- schoology
- Student Privacy Pledge
- Titan School Solutions
- Tools4Ever
- Signal Ki
- Matomo
- LivingTree

Product Data List


The data your Educational Institution stores on Aeries' systems may include, but is not limited to, the following information about students and their guardians:

- Demographic information such as name, mailing address, email address, and date of birth;
- Student education records including, but not limited to student's grades, class enrollment, and behavioral records;
- Financial information, including but not limited to fees and fines, such as Chromebook insurance, or administrative fees, determined by LEAs;
- Health-related information including your student's immunizations and vision and hearing screening results;
- System usernames and passwords.

Accuracy Statement

Aeries Software, Inc. hereby confirms the accuracy and truthfulness of all information contained in the Aeries Software, Inc. profile and has authorized iKeepSafe to make the profile available to any interested schools.

Signed and agreed:




(Signature)

James Mallory
Vice President of Operations
Aeries Software, Inc.,
770 The City Drive South, Suite 6500
Orange, CA 92868
888-487-7555
Legal@aeries.com.

07/29/2024

The Aeries service has been reviewed and found in alignment with iKeepSafe's FERPA and California Privacy Program Guidelines as indicated by this product profile. Aeries Software, Inc. has been awarded the iKeepSafe FERPA and California Privacy Program badges.

DocuSigned by:

4936610B3023488...

(Signature)

Amber Lindsay
President & CEO
iKeepSafe

07/29/2024

Copyright

© 2018 Internet Keep Safe Coalition (iKeepSafe). All rights reserved. iKeepSafe's California Privacy Assessment Program™ materials have been developed, copyrighted, and distributed for incidental, classroom use only. iKeepSafe's copyright notice and distribution restrictions must be included on all reproductions whether in electronic or hard copy form. These materials are intended to convey general information only and not to provide legal advice or any other type of professional opinion.

Disclaimer

¹By using the California Privacy Assessment Program or accepting any materials related to the California Assessment Program, you expressly acknowledge and agree that neither Internet Keep Safe Coalition, their affiliates, subsidiaries, or designees nor each of their respective officers, directors, employees or agents (collectively, Associates), can guarantee, certify or ensure that you are in compliance with FERPA, SOPIPA, California AB 1584, or any other state or federal laws. You understand that the California Privacy Program does not constitute legal or any other type of professional advice and the California Privacy Seal is not a legal determination.