



iKeepSafe Product Profile *SchoolMint Software, Inc.* *HERO*

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 HERO complies with FERPA, SOPIPA and CSPC. It indicates that HERO has been assessed for alignment with the iKeepSafe Program Guidelines.

Product Overview

HERO helps school systems streamline and transform their entire student enrollment experience.

HERO software streamlines all aspects of their student enrollment process – student recruitment, application and lottery management, registration, school choice and unified enrollment, family communications, and year-round digital forms.

Available online and on mobile devices, HERO's user friendly design and seamless data integration with leading student information systems (SIS) transform the end-to-end enrollment experience for school staff and parents

Agreement

A. As related to the Family Educational Rights and Privacy Act (“FERPA”) (20 U.S.C. Section 1232g), HERO agrees:

1. Student records obtained by HERO 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 HERO.
2. HERO users may retain possession and control of their own generated content.
3. HERO will not use any information in a student record for any purpose other than those required or specifically permitted by the HERO 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, HERO users may access, correct, update, or delete personal information in their profile by signing into HERO, accessing their HERO account, and making the appropriate changes.
5. HERO 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, HERO will promptly notify users unless specifically directed not to provide such notification by law enforcement officials.
7. HERO 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. HERO agrees to work with educational institutions 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. HERO prohibits using personally identifiable information in student records to engage in targeted advertising.
10. HERO 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.

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

Prohibitions:

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

Obligations:

1. HERO is committed to maintaining the security and confidentiality of pupil records as noted herein.
2. HERO will delete student information when requested by the school district.
3. HERO will disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

C. As it relates to California AB 1584 (Buchanan) Privacy of Pupil Records: 3rdParty Digital Storage & Education Software (Education Code section 49073.1)

1. Pupil records obtained by HERO from LEA continue to be the property of and under the control of the LEA.
2. HERO does not provide a platform by which pupils can create content ; therefore, HERO does not provide a means by which pupils may retain possession and control of such content.
3. HERO will not use any information in pupil records for any purpose other than those required or specifically permitted by the HERO Service Agreement.
4. Parents, legal guardians, or eligible pupils may review personally identifiable information in the pupil’s records and correct erroneous information by contacting the educational institution. District personnel have direct access via the HERO product account login to review pupil data. HERO will provide clients with a copy of pupil data, and will modify and/or delete upon written request by the LEA.
5. HERO is committed to maintaining the security and confidentiality of pupil records. To that end, HERO has taken the following actions: (a) limiting employee access to student data based on roles and responsibilities; (b) conducting background checks on employees who have access to student data; (c) conducting privacy training that includes FERPA for employees with access to

- pupil data; (d) protecting personal information with technical, contractual, administrative, and physical security safeguards in order to protect it from unauthorized access, release or use.
6. In the event of an unauthorized disclosure of a pupil's records, HERO will promptly notify the educational institution unless specifically directed not to make such notification by law enforcement. The notification will include: date of the breach, the types of information that were subject to the breach; general description of what occurred; steps the HERO is taking to address the breach; the contact person at the vendor who the data holder can contact. HERO will keep the client District fully informed until the incident is resolved.
 7. HERO will delete personally identifiable data upon request of the LEA and/or upon expiration of the services agreement. All data is deleted within 60days of expiration of services agreement.
 8. HERO agrees to work with the LEA 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 pupil records and to correct any inaccuracies therein as described in statement 4 above.
 9. HERO prohibits using personally identifiable information in pupil records to engage in targeted advertising.

Data Review Process

HERO provides users direct access to the personally identifiable information that they provide to HERO through product functionality. Users also have the ability to contact HERO for access to all personal information on file by contacting HERO through support@schoolmint.com.

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

General inquiries related to privacy may be directed to:

SchoolMint, Inc.

Privacy Director HERO
564 Market St #500
San Francisco, CA 94104
(844) 287-2466

support@HERO.com

Security Protocols

HERO 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 HERO APIs and never stored on any intermediate server.

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

HERO uses AWS Data Centers and these centers conform to the following:

AWS is a secure, durable technology platform with industry-recognized certifications and audits: PCI DSS Level 1, ISO 27001, FISMA Moderate, FedRAMP, HIPAA, and SOC 1 (formerly referred to as SAS 70 and/or SSAE 16) and SOC 2 audit reports. Their services and data centers have multiple layers of operational and physical security to ensure the integrity and safety of your data.

Please see more information below in the available link:

Amazon Web Services (AWS) <https://aws.amazon.com/security/>

Personnel

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

Training: Employees of HERO 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, HERO will provide schools with:

- audit rights to the school's data
- access to the results of HERO' or its third-party security audit

Data Breach

In the event of an unauthorized disclosure of a student's records, HERO 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 HERO 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 HERO has taken or shall take to prevent future similar unauthorized use or disclosure; and
- g. who at HERO the user can contact. HERO will keep the user fully informed until the incident is resolved.

HERO 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

HERO states they will retain personal identifiable information for as long as the account is active, or as needed to provide their users with their services. Please contact them at the email address at support@schoolmint.com should someone wish to cancel their account or request that we no longer use the information to provide services. They will retain and use the information as necessary to comply with their legal obligations, resolve disputes, and enforce their agreements.

Research

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

Additionally, as part of this use of information, they may provide aggregate information to partners about how our users, collectively, use our site. They may share this type of statistical data so that their partners also understand how often people use their partners' services and the Website to help provide the user with an optimal online experience.

Third Parties

HERO 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.

HERO 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. HERO 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 HERO' data privacy and security policies and expectations.

HERO utilizes the following third-party vendors:

Provider	How HERO uses the Provider	What information is shared
AWS	Data Storage	
Google Analytics	Analytics	
Full Story		
Totango		
Mixpanel	Analytics	


Product Data List

Data Collected	General Purpose of Data Collection
STUDENT FIRST AND LAST NAME	Required to support product functionality
STUDENT PHYSICAL ADDRESS	Required to support product functionality
STUDENT PHONE/Mobile NUMBER	Required to support product functionality
STUDENT SOCIAL SECURITY NUMBER	Required to support product functionality
STUDENT AGE/DOB	Required to support product functionality
STUDENT ETHNICITY	Required to support product functionality
STUDENT GENDER	Required to support product functionality
OTHER STUDENT ID	
PARENT FIRST AND LAST NAME	Required to support product functionality
PARENT PHYSICAL ADDRESS	Required to support product functionality
PARENT PHONE/MOBILE NUMBER	Required to support product functionality
PARENT EMAIL ADDRESS	Required to support product functionality
SCHOOL NAME	Required to support product functionality
SCHOOL ADDRESS	Required to support product functionality
Grades	Required to support product functionality
PHOTOGRAPH,VIDEOOR AUDIO FILE	Required to support product functionality
ACCESS TIME	Analytics
TIME SPENT ON SITE	Analytics
PAGE VIEWS	Analytics
REFERRING URLS	Analytics

Accuracy Statement

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

Signed and agreed:

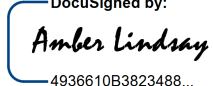


(Signature)

Casey Bienvenu
1100 Bertrand Dr.
Lafayette, LA 70506
(844) 287-2466

02/07/2022

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

DocuSigned by:

4936610B3823488...

(Signature)

Amber Lindsay
President & CEO
iKeepSafe

02/07/2022

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.