



iKeepSafe Product Profile HERO K12

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 K12 complies with FERPA and CSPC. It indicates that HERO K12 has been assessed for alignment with the iKeepSafe Program Guidelines.

Product Overview

HERO K12

Hero is a behavior tracking solution for schools and school districts, allowing school staff to record and apply policies to student behavior, analyze that data, and inform parents about student conduct.

<https://www.herok12.com/>

Agreement

As related to the Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. Section 1232g), HERO K12 agrees:

1. Student records obtained by HERO K12 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 K12
2. HERO K12 users may retain possession and control of their own generated content.
3. HERO K12 will not use any information in a student record for any purpose other than those required or specifically permitted by the HERO K12 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 K12 users may access, correct, update, or delete personal information in their profile by signing into HERO K12, accessing their HERO K12 account, and making the appropriate changes.
5. HERO K12 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 K12 will promptly notify users unless specifically directed not to provide such notification by law enforcement officials.
7. HERO K12 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 K12 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. HERO K12 prohibits using personally identifiable information in student records to engage in targeted advertising.
10. HERO K12 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"), HERO K12 agrees:

1. HERO K12 does not target advertising via the HERO K12 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 K12 does not use information, including persistent unique identifiers, created or gathered by the HERO K12 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 K12 does not and will not sell, rent, or otherwise provide personally identifiable information to any third party for monetary gain.
4. HERO K12 does not disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

Data Review Process

HERO K12 provides users direct access to the personally identifiable information that they provide to HERO K12 via product functionality. Users also have the ability to contact HERO K12 for access to all personal information on file by contacting HERO K12 through support@herok12.com

We have added to the HERO K12 Privacy Policy:

Your Educational Agency uses HERO K12 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 Agency and are governed by the contract between HERO and your Educational Agency.

Your Educational Institution determines the information collected, maintained, and processed using HERO services. If you have any questions regarding the collection, storage, and use of the information your Educational Institution shares with HERO, please contact your Educational Institution directly.

General inquiries related to privacy may be directed to:

HERO K12
1501 NW 163rd Street
Miami, FL 33169
Phone (800) 396-1615
email: support@herok12.com

Security Protocols

HERO K12 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

Data is transferred using HTTPS.

Data at Rest

Key data, specifically PII, in non-production environments is depersonalized. HERO servers on AWS and are on a VPC (virtual private cloud) which prevents unauthorized access. Also, we access our servers and databases on VPC through VPN (jumpbox), providing additional layer of security on top of a secure VPC.

Data Center Security

HERO K12 uses AWS Data Centers and these centers conform to the following:

AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, and 27018:2014.

<https://aws.amazon.com/compliance/iso-27001-faqs/>

<https://aws.amazon.com/about-aws/whats-new/2011/11/11/aws-publishes-new-service-organization-controls-1-report/>

AWS aligns with the CSA STAR Attestation and Certification based on the determinations in our third-party audits for System and Organization Controls (SOC) 2 Reports and ISO 27001:

<https://aws.amazon.com/compliance/csa/>

Personnel

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

Training: Employees of HERO K12 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.

Access to Audit

Once per year, HERO K12 will provide schools with:



audit rights to the school's data



access to the results of HERO K12' or its third-party security audit

Data Breach

In the event of an unauthorized disclosure of a student's records, HERO K12 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 K12 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 K12 has taken or shall take to prevent future similar unauthorized use or disclosure; and
- g. who at HERO K12 the user can contact. HERO K12 will keep the user fully informed until the incident is resolved.

HERO K12 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 K12 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 support@herok12.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

HERO K12 stated; We use none of the customer data for research or statistical purposes at this time.

They use de identified data for usage patterns and for product design purposes.

Third Parties

HERO K12 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 K12 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 K12 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 K12' data privacy and security policies and expectations.

HERO K12 utilizes the following third-party vendors:

Google Analytics -- Internal Product Analytics -- Depersonalized Usage Data

WalkMe -- Self-service support -- Send unique user IDs

Gainsight -- Internal Product Analytics -- Usage Data and School Staff Account Info

ZenDesk -- Support Helpdesk & Chat -- Send usernames, names, UGC

Intercom -- Internal Product Analytics -- User Usage Data

SIS Vendors, Clever -- District/School Data Flow

Inflow: Student, User, and Rostering information

Outflow (optional): Behavior records

AWS -- Data storage and processing

Product Data List

Use of Information Collected: This was added and/or modified to the TOS/PP section:

We use Data About Our Customers to perform the Services requested. For example, data collected from schools regarding school schedules and student information is required to promote students good behavior and provides a standardized process for Student disciplinary actions. Also, if you fill out a "Contact Me" Web form, we will use the information provided to contact you about your interest in the Services.

Data collected from Parents regarding messages sent to schools is to facilitate communication between school and parents and have a better parent engagement.

	DATA Collected for Operation	General Purpose of Data Collected
1	STUDENT FIRST AND LAST NAME	Required to support Product Functionality

2	STUDENT PHYSICAL ADDRESS	Required to support Product Functionality
3	STUDENT EMAIL ADDRESS	Required to support Product Functionality
4	STUDENT PASSWORD	Required to support Product Functionality
5	STUDENT ID	Required to support Product Functionality
6	STUDENT AGE/DOB	Required to support Product Functionality
7	STUDENT ETHNICITY	Required to support Product Functionality
8	STUDENT GENDER	Required to support Product Functionality
9	STUDENT GRADE	Required to support Product Functionality
10	STUDENT LANGUAGE	Required to support Product Functionality
11	PARENT FIRST AND LAST NAME	Required to support Product Functionality
12	PARENT PHYSICAL ADDRESS	Required to support Product Functionality
13	PARENT PHONE/MOBILE NUMBER	Required to support Product Functionality
14	PARENT EMAIL ADDRESS	Required to support Product Functionality
15	PARENT PASSWORD	Required to support Product Functionality
16	SCHOOL NAME	Required to support Product Functionality
17	SCHOOL ADDRESS	Required to support Product Functionality
18	TEAMS/CLUBS	Required to support Product Functionality
19	PHOTOGRAPH,VIDEO OR AUDIO FILE	Required to support Product Functionality
20	VEHICLE INFORMATION	Required to support Product Functionality
21	BEHAVIOR ENTRIES - ACTION, ACTION DATA	Required to support Product Functionality.
22	CLASSROOM INFORMATION - PERIOD, INSTRUCTOR, STUDENTS IN THE CLASS	Required to support Product Functionality

Accuracy Statement

HERO K12 hereby confirms the accuracy and truthfulness of all information contained in the HERO K12 profile and has authorized iKeepSafe to make the profile available to any interested schools.

Signed and agreed:



(Signature)


Matthew Poirier,
CTO SchoolMint.

HERO K12

1100 Bertrand Drive, Suite B
Lafayette, LA 70506
phone: (800) 396.1615
info@schoolmint.com

10/20/2020

The HERO K12 service has been reviewed and found in alignment with iKeepSafe's FERPA and California Privacy Program Guidelines as indicated by this product profile. HERO K12 has been awarded the iKeepSafe FERPA and California Privacy Program badges.

DocuSigned by:

4936610B3823488...

(Signature)

Amber Lindsay
President & CEO
iKeepSafe

10/30/2020

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

By 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.