iKeepSafe Product Profile
Rhithm, 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 Rhithm complies with, FERPA, SOPIPA, California AB 1584, and other California state laws and district policies. It indicates that Rhithm has been assessed for alignment with the iKeepSafe FERPA and California Privacy Program Guidelines.

Product Overview

Rhithm is a wellness check-in tool. The platform selects an ideal 1-2 minute activity video to regulate well-being based on user given data from a simple emoji assessment. This data is available on dashboards to reflect and connect with as desired at the campus, district/network and state levels.

https://rhithm.app/

Agreement

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

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

Prohibitions:

1. Rhithm does not target advertising via the Rhithm 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. Rhithm does not use information, including persistent unique identifiers, created or gathered by the Rhithm service to amass a profile about a K–12 student, their families/guardians or educators except in furtherance of K–12 school purposes.

3. Rhithm does not and will not sell, rent, or otherwise provide personally identifiable information to any third party for monetary gain.

4. Rhithm does not disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

Obligations:

5. Rhithm is committed to maintaining the security and confidentiality of pupil records as noted herein.

6. Rhithm will delete student information when requested by the school district.

7. Rhithm will disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

Data Review Process

Rhithm provides users direct access to the personally identifiable information that they provide to Rhithm via product functionality. Users also have the ability to contact Rhithm for access to all personal information on file by contacting Rhithm through team@rhithm.app.

You can also ask us to correct any information we hold about you that is inaccurate. If you would like us to send you a copy of your information or correct your information, please email us at team@rhithm.app.

You can also ask us to delete your account and all the associated personal data held by Rhithm by emailing us at team@rhithm.app

If you are a school, you may request to review your students' information, have it deleted, and refuse further data collection by emailing us at team@rhithm.app . If further data collection is stopped, those individuals may no longer be able to use Rhithm.

General inquiries related to privacy may be directed to:

Data Governance Officer at team@rhithm.app
100 W. Oak St #G-106, Denton, TX 76201
940-268-1029

Security Protocols

Rhithm 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:

HTTPS encrypted

Data at Rest:

Rhithm data storage providers provide an Encryption methodology that is inherent in their data storage systems and is replicated in encrypted form for backup and disaster recovery.

Data Center Security:

Rhithm 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 Rhithm will receive annual privacy and security training that includes FERPA and CSPC.

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, Rhithm will provide schools with:

[X] audit rights to the school's data

[X] access to the results of Rhithm or its third-party security audit

Data Breach

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

Rhithm 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

Rhithm states they will not keep your information for longer than we need to for the purposes listed in this policy.

If you use an account through your school or school district and you wish to close your account with one of our Services, please contact your school or school district and at their direction we will remove your Personal Information and Profile, if applicable, from the active databases for the Service(s) you request through your school or school district. Please let your school or school district know which Service(s) you wish to close.

Research

Rhithm may use data which has been de-identified and/or aggregated for product development, research, analytics and other purposes, including for the purpose of analyzing, improving, or marketing the Services.

Third Parties

Rhithm 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.

Rhithm 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. Rhithm 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 Rhithm's data privacy and security policies and expectations.

Rhithm utilizes the following third-party vendors:

https://rhithm.app/wp-content/uploads/2021/02/Rhithm-3rd-Parties-List-1.pdf

Product Data List:

Data Collection:

STUDENT FIRST AND LAST NAME	Rostering the application
STUDENT PHYSICAL ADDRESS	Rostering the application
STUDENT EMAIL ADDRESS	Rostering the application
OTHER STUDENT ID	Rostering the application
STUDENT AGE/DOB	Rostering the application
STUDENT ETHNICITY	Rostering the application
STUDENT GENDER	Rostering the application
SCHOOL NAME	Rostering the application
SCHOOL ADDRESS	Rostering the application
OTHER PERSISTENT IDENTIFIER	To support Product Functionality
Well-Being Data	To support Product Functionality

Accuracy Statement

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

Signed and agreed:

DocuSigned by:
Josh Knutson
207B2AAEA7E2498...
(Signature)

Josh Knutson
Rhithm, CEO/Co-Founder
josh@rhithm.app
214.762.0439

12/13/2022

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

DocuSigned by:
Amber Lindsay
4936610B3823488...
(Signature)

Amber Lindsay
President & CEO
iKeepSafe

12/13/2022

Copyright

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.