iii iKeepSafe

Introduction

The iKeepSafe California 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 Stemify Service complies with FERPA. It indicates that the Stemify Service has been assessed for alignment with the iKeepSafe FERPA Privacy Program Guidelines.

The iKeepProfile is not legal guidance, nor does it guarantee or otherwise assure compliance with any federal or state laws. If you have questions on how to use the iKeepProfile to support your school's compliance efforts, please contact your school attorney.[1]

Product Overview

Stemify: https://stemify.ai/

SaaS-based STEM Platform for Adaptive Instruction and Learning for STEM success.

The Stemify Platfrom: An end to end STEM focused platform built to help teachers and students realize their full potential.

Create & Deploy Assessments:

Create and deploy assessments for your students using our flexible and intuitive interface. Create questions, question pools and multiple versions of assessments with the ability to tag any item with key topics that will tie into our AI engine.

Analyze & Report:

Stemify provides an array of reporting tools that analyze the interaction of the students with the platform and its content to map cognitive and non-cognitive factors that affect students' performance across different core math concepts.

1

Engage With Video Content:

Use our existing library of foundational math to Calculus or build your own learning modules of videos, quizzes and practice assignments to build your own library of content for your students.

AI Personalization:

Using advanced IRT psychometric techniques and distractor analysis, the platform provides a personalized study plan for each student, helping them retain and recall concepts in foundational mathematics.

Agreement

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

1. Student records obtained by Stemify 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 Stemify.
2. Stemify users may retain possession and control of their own generated content.
3. Stemify will not use any information in a student record for any purpose other than those required or specifically permitted by the Stemify 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.
5. Stemify 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 have 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, Stemify will promptly notify users unless specifically directed not to provide such notification by law enforcement officials.
7. Stemify 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. Stemify 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.

2

9. Stemify prohibits using personally identifiable information in student records to engage in targeted advertising.
10. Stemify 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.

Data Review Process

Parents are encouraged to work directly with teachers and school to make any changes in your data. If however, you need to get in touch with us, you can write to support@stemify.ai and we will work with the school and do our best to make the required changes.

Teachers, administrators and Students can directly edit their information in their Stemify profiles. Schools also have a right to use any other similar service and can place a request to get all of their data. We will do our best to comply with such requests.

You may also send requests about your Personal Information, including changes to your contact preferences, and changes to or deletions of your information or content you post, by emailing support@stemify.ai

General inquiries related to privacy may be directed to:

Please contact us at the following with any questions about this Privacy Policy:

STEMIFY, Inc.
400 Farmington Ave.
Farmington, CT 06032
support@stemify.ai

Security Protocols

Stemify has a comprehensive Information Security Program in place that ensures the confidentiality, integrity and availability of systems, networks and data. The following is a general overview of data security protocols:

Data In Transit:

Stemify uses both SFTP and HTTPS depending on client needs. All data transferred HTTPS is with the approved SSL encryption strategies recommended by AWS

3

Data at Rest:

AWS Storage Gateway uses SSL/TLS (Secure Socket Layers/Transport Layer Security) to encrypt data that is transferred between the gateway appliance and AWS storage. By default, Storage Gateway uses Amazon S3-Managed Encryption Keys (SSE-S3) to server-side encrypt all data it stores in Amazon S3.

Data Storage:

Data is stored in AWS S3 Database), which is encrypted.

Data Center Security:

Stemify utilizes data centers operated by Amazon Web Services (AWS) which has extensive experience in designing, construction, and operation large-scale data centers. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at the building ingress points by professional security staff utilizing video surveillance, intrusion detection system and other electronic means. Authorized staff must pass a two-factor authentication a minimum of two times to access data center floors. AWS only provides data center access and information to employees and contracts who have a legitimate business need.

Personnel :

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

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

[X]   audit rights to the school's data

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

4

Data Breach

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

Stemify will <u>notify</u> 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

Stemify 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@stemify.ai 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

 Stemify collects data on student assessment and practice assignment performance (correct vs incorrect responses, time taken to complete assessments/assignments) to understand trends in student learning to continually improve the product.

This information of Student'sl Personally Identifiable Information (PII) is stripped from the data file including First Name, Last Name, and email address.

Stemify does not use end user data in any non-production environments including testing, development and training. Stemify does not use end user data for production improvement or research. Stemify only uses end user data to debug customer specific issues.

Third Parties

Stemify 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.

Stemify 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. Stemify 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. Stemify utilizes the following third party vendors as indicated below

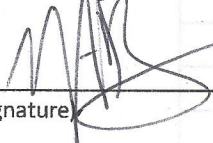| Third Party	Business function or Service
Amazon Web Services (AWS)	Cloud hosting Platform
Google Analytics	Analytics

Product Data List

#	Data Collected for Operation	General Purpose of Data Collection
1	Student, Faculty, Admin: First and Last Name	Required to support product functionality
2	Student, Faculty, Admin: Email Address	Required to support product functionality
3	Student, Faculty, Admin: School ID	Required to support product functionality
4	Access Time	Business Intelligence
5	Time Spent on Site	Business Intelligence
6	Page Views	Business Intelligence
7	Referring URLS	Business Intelligence

Accuracy Statement

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

Signed and agreed:

_____
(Signature)

Nick Bequary
COO
STEMIFY, Inc.
400 Farmington Ave.
Farmington, CT 06032

09/4/2020

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

Amber Lindsay
4936610B3823488...
(Signature)

Amber Lindsay
President & CEO
iKeepSafe

09/04/2020

8