iKeepSafe Product Profile
Splash Learn

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

Product Overview

Splash Learn: https://www.splashlearn.com/

StudyPad's vision is to transform K-12 learning by making it fun and personalized for every child and to prepare them for skills required in the 21st-century. StudyPad is uniquely poised to harness the rapid growth in the education technology space using the backdrop of the ubiquitous adoption of smartphones, tablets, AR and VR.

StudyPad's flagship product SplashLearn is transforming the way elementary school children in grades K-5 learn and study math through a highly engaging, and personalized program. SplashLearn is available across all digital platforms (iOS, Desktops, Android) and has been used by more than 30 Million students worldwide. It has won many awards and has been featured by Apple multiple times.

Agreement

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

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

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

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

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

Data Review Process

Splash Learn provides users direct access to the personally identifiable information that they provide to Splash Learn via product functionality. Users also have the ability to contact Splash Learn for access to all personal information on file by contacting Splash Learn through compliance@splashlearn.com

Review and update your data: You have the right to access and update any personal data that we have collected. Some personal data, such as the account holder's name and email address can be found and updated using the account management tools on our website at https://www.splashmath.com/profile. For any personal data beyond this, please submit a request using the contact information at the end of this section. We may request more information to confirm your identity before modifying any personal data.

General inquiries related to privacy may be directed to:

StudyPad, Inc.
Joy Deep Nath
548 Market, St #64304
San Francisco CA - 94104
Phone: +1 855 979 8948

Email support: compliance@splashlearn.com

Security Protocols

Splash Learn 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.

Securing data in transit: AWS

Data encryption helps prevent unauthorized users from reading data on a cluster and associated data storage systems. This includes data saved to persistent media, known as data *at-rest*, and data that may be intercepted as it travels the network, known as data *in-transit*.

Beginning with Amazon EMR version 4.8.0, you can use Amazon EMR security configurations to configure data encryption settings for clusters more easily. Security configurations offer settings to enable security for data in-transit and data at-rest in Amazon Elastic Block Store (Amazon EBS) storage volumes and EMRFS on Amazon S3.

Data at Rest

Splash Learn' data storage is provided by AWS.

Our main data store has at rest encryption (AES 256). We are in the process of having at rest encryption on the transitional data stores as well (caches)

Data Center Security

Splash Learn uses AWS as a Data Storage Provider:

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

Personnel

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

Training: Employees of Splash Learn 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, Splash Learn will provide schools with:

[X] audit rights to the school's data

[X] access to the results of Splash Learn' or its third-party security audit

Data Breach

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

Splash Learn 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,

See: Splash Learn Privacy Policy https://www.splashlearn.com/privacy

Data Deletion

Splash Learn Data Deletion and Retention Policy described below from Privacy Policy:

Home Accounts: For accounts created by parents, if neither the student, nor the student's parent(s) or any of the other student accounts associated with the parents' accounts have logged into their account in 2 years, Splash Learn will automatically delete or de-identify the personal information tied to the student account that is not necessary for educational purposes or legal obligations, including device tokens, device identifiers and IP addresses. In effect, the student account will be anonymized and de-linked from the parent account and the data will be non-recoverable. We will make reasonable attempts to inform parents about the account modification a few days in advance. We may retain some personal information about the parents for reasons outlined earlier, but these will not be tied to any personal information about the student. Parents can always request deletion of their accounts as outlined in the "Deleting your account" section.

Classroom Account: If neither the teacher, nor any of the students associated with the teacher account have logged into their account in 2 years or performed any activity, Splash Learn automatically deletes or de-identifies any personal information tied to the student accounts that is not necessary for educational purposes or legal obligations, including device tokens, device identifiers and IP addresses.

What happens when an account is deleted: Splash Learn de-identified or deletes any personal information tied to the accounts, including emails, usernames. device token, device identifiers, IP addresses. This information may persist in backups that we maintain, for a reasonable amount of time. Splash Learn retains de-identified usage information about the accounts unless we contractually obligated to delete such information.

When a teacher or school administrator deletes an account from within their Splash Learn dashboard, the deleted accounts are kept in a recoverable state for 14 days before the deletion actually takes place. This is done so that any erroneous deletions on the user's part can be recovered and accounts may be restored.

Please note that after an account is deleted from our systems, it is not possible for us to restore the account or any personal information associated with it.

Research

Please see policy statement on research for Splash Learn:

Personal Information Collected Automatically

We receive and store certain types of information whenever you interact with our Services or use our services. Company automatically receives and records information on our server logs from your browser including your IP address, cookie information, and the page you requested. Generally, our service automatically collects usage information, such as the numbers and frequency of visitors to our Services and its components, similar to TV ratings that indicate how many people watched a particular show. Company only uses this data in aggregate form, that is, as a statistical measure, and not in a manner that would identify you personally. This type of aggregate data enables us to figure out how often customers use parts of the Services so that we can make the Services appealing to as many customers as possible and improve those Services. As part of this use of information, we may provide aggregate information to our partners about how our customers, collectively, use our Services. We share this type of statistical data so that our partners also understand how often people use the Services, so that they, too, may provide you

with an optimal online experience. Again, Company does not disclose aggregate information to a partner in a manner that would identify you personally.

We never share that Children's Personal Information with any third party. A child's usage data (i.e. performance on tests, games, etc. available on the Services) is shared through aggregated, anonymous comparisons, but never in a way that could personally identify the child.

Third Parties

Splash Learn 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.

Splash Learn 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. Splash Learn 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 Splash Learn' data privacy and security policies and expectations.

Splash Learn utilizes the following third-party vendors:

Third Party	**Purpose**	**Data Shared**
Stripe	Product Purchase (Payment gateway)	Credit Card Information, IP Address
Xero	Invoicing for schools	Teacher Email, Address, Name, Product Details
Customer Communications		
Mailchimp	Marketing Communications	Email, Email Content, Email tracking
Sendgrid	Product Updates, Marketing Communications	Email, survey answers, Email tracking
Survey Monkey	Surveys	Email, survey answers, Email tracking
Mailgun	Marketing Communications	Email, survey answers, Email tracking
Moengage	Marketing Communications	Email, Email Content, Email tracking
Amazon SNS	Sending push notifications	Device Token
Close.io	CRM tool used to send promotional emails, making sales calls, managing sales pipeline, account management	Email, Name, Phone no, School Address
Drift	Parent Chat with Math Coach	Email, Phone no, Grade
Google Calendar	Scheduling	Email, Name and Phone no
Calendly	Scheduling calls for	Email, Phone no, Name

	parents/teachers	
Google Hangouts	Sales, Product Service	Information shared by the customer including email address and name
Zoom	Sales, Product Service	Information shared by the customer including email address and name
Customer Support		
Uservoice	Customer Support	Information shared by the customer including email address and name
Zendesk	Customer Support	Information shared by the customer including email address and name
Freshdesk	Customer Support	Information shared by the customer including email address and name
Facebook	Customer Support - Addressing user concern	Information shared by the customer including email address and name
Analytics and Visualization		
Google Analytics	Product Analytics	Anonymous usage information (No PII)
Mixpanel	Product Analytics	Anonymous usage information (No PII)
Hotjar	Surveys and Analytics	Email when shared by customer through surveys
Adjust	Campaign Attribution (Android Only)	Android Ad Identifier, Device Indentifier
Stitch	Analytics Data Aggregation	Anonymous analytics data collected from different sources
Looker	Analytics	All channels analytics data, data resides on SplashLearn servers
Google Optimize	AB Testing	Google Analytics Data
Google Data Studio	Data Visualisation	Google Analytics Data
Technical Tools and Services		

Amazon Web Services	Website Hosting, Databases	All data, logs and applications reside here
Airbrake	Error Monitoring	IP, Email, or other other customer data may be present as part of error reporting
New Relic	Application Performance Monitoring	Anonymized IP not linked to any customer
Google Firebase	Application Performance Monitoring	Anonymized IP not linked to any customer
Facebook App SDK	Authentication (Signup)	Install Event
Internal Workflow/communication Tools		
Zapier	Automation and work flow tool	Email, Phone no, Grade, Name
Slack	Internal Communications	May have user email for internal communication
Atlassian Jira	Project Management	May have user email / for support tickets
Advertising		
Google Ads	Customer Acquisition and Ad Measurement	Anonymous/ Aggregate information (click / conversions count) , User Browser Signature
Bing Ads	Customer Acquisition and Ad Measurement	Anonymous/ Aggregate information (click / conversions count) , User Browser Signature
Facebook ads	Customer Acquisition and Ad Measurement	Anonymous/ Aggregate information (click / conversions count) , User Browser Signature
Google Double Click (DV360)	Customer Acquisition and Ad Measurement	Anonymous/ Aggregate information (click / conversions count) , User Browser Signature
Search Ads HQ	Customer Acquisition and Ad Measurement	Anonymous/ Aggregate information (click / conversions count) - No user data

Product Data List

Data Collection for Splash Learn from Policy below:

We receive and store any information you enter on our Services or provide to us in any other way. The types of Personal Information collected include your full name, email address, ZIP code, credit card and/or other payment information, Children's Personal Information (which is limited to the child's name and gender), IP address, browser and location information, username, password and any other information necessary for us to provide our services. We also offer users the ability to sign up for the Services using their existing Facebook or Google account. If you choose to sign up for the Services using one of these accounts, we will receive your full name from the service provider managing that account.

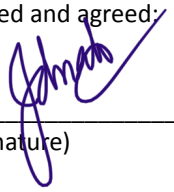
If you are using the service as an Educational Institution, Student information may be visible during Customer Support and/or Troubleshooting. Personally identifiable information such as Student Name, Teacher Email Address, login dates and times could be viewed on our service by Product Support Staff.

#	**DATA Collected for Operation**	**General Purpose of Data Collected**
1	STUDENT FIRST AND LAST NAME	Required to support Product Functionality
2	STUDENT PASSWORD	Required to support Product Functionality
3	STUDENT ID (username)	Required to support Product Functionality
4	STUDENT GENDER	Analytics
5	STUDENT LANGUAGE	Required to support Product Functionality
6	PARENT EMAIL ADDRESS	Survey and Communications
7	PARENT PASSWORD	Required to support Product Functionality
8	SCHOOL NAME	CRM for Sales/Communication
9	SCHOOL ADDRESS	CRM for Sales/Communication
10	GEOLOCATION DATA	Analytics
11	BROWSER TYPE	Analytics
12	ACCESS TIME	Analytics
13	TIME SPENT ON SITE	Analytics
14	PAGE VIEWS	Analytics
15	REFERRING URLS	Analytics
16	Zip Code (Teacher)	Analytics
17	Teacher Phone Number	CRM for Sales/Communication
18	Device Id	Analytics
19	Device Information: Model No., OS version, Platform , Manufacturer	Analytics

Accuracy Statement

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

Signed and agreed:



(Signature)

Joy Deep Nath
Co-Founder
Splash Learn
09/23/2022

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

DocuSigned by:
Amber Lindsay
4036610B3823488...

(Signature)

Amber Lindsay
President & CEO
iKeepSafe

09/23/2022

Copyright

Disclaimer

[1] 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.