iKeepSafe

iKeepSafe Product Profile
ClassTag

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 ClassTag complies with FERPA. It indicates that ClassTag has been assessed for alignment with the iKeepSafe Program Guidelines.

Product Overview

ClassTag is a service that helps teachers to communicate and coordinate with parents, while getting free stuff for their classroom

Below are some of the features of ClassTag:

Direct messaging by email and text

School or class-wide announcements

Photo and video sharing

Volunteer signups, donations and supply lists

Parent-teacher conference scheduling

Class calendar and events

Newsletters

https://home.classtag.com/

Agreement

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

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

ClassTag provides the ability to make changes to your information, including accessing, correcting or updating your information, through your registered account or by emailing us at support@classtag.com. A school may request (or a parent, legal guardian, caregiver or teacher may request that the applicable school make a request) to review, to have corrected or updated or to cease further use or collection of content or information relating to a student by contacting us via live chat during regular business hours on the Service or via email at support@classtag.com. A parent or legal guardian can remove a student from the Service and this will result in no further collection or use of content or information from such student.

General inquiries related to privacy may be directed to:

ClassTag
235 West 48 th Street, #43C
New York, New York 10036.

Email address: support@classtag.com.

Security Protocols

ClassTag 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

AES-256 is used as the data encryption technique. 256-bit encryption is a data/file encryption technique that uses a 256-bit key to encrypt and decrypt data or files.

Data Center Security

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

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.

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 ClassTag 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, ClassTag will provide schools with:

☒ audit rights to the school's data

☒ access to the results of ClassTag' or its third-party security audit

Data Breach

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

ClassTag will notify impacted user (s) within a reasonable period of time following the discovery of a breach of security that results in the unauthorized release, disclosure or acquisition of student information, and any acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by ClassTag.

Data Deletion

At ClassTag you can delete your information through your registered account or by emailing us at support@classtag.com. A school may request (or a parent, legal guardian, caregiver or teacher may request that the applicable school make a request) to have deleted or de-identified content or information relating to a student by contacting us via live chat during regular business hours on the Service or via email at support@classtag.com. We will retain such content or information that is deleted or de-identified for as long as reasonably necessary for the purposes described in this Privacy Policy or the Terms, while we have a business need to do so in connection with your registered account or as required by law (for example, for legal, tax, accounting or other purposes), whichever is the longer.

Research

ClassTag stated we use de identified data for usage patterns and for product design purposes.

Third Parties

ClassTag 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.

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

ClassTag utilizes the following third-party vendors:

1) Airbrake [link: https://airbrake.io/privacy] for error monitoring

Info shared: Event and user data associated with errors on the Service

2) Amazon [link:

https://www.amazon.com/gp/help/customer/display.html?ie=UTF8&amp;nodeId=468496&amp;ref

_=footer_privacy] for network infrastructure, photo and video encoding, data storage

Info shared: Media files

3) Google [link: https://policies.google.com/privacy] Google Analytics for Service analytics,

Google Cloud for language translations, Google G Suite for internal data storage,

Google Marketing Platform for managing javascript on the Service

Info shared: Service usage and IP address for Google Analytics and Google Marketing

Platform, User-generated content for Google Cloud, Internal emails, files, documents,

etc. for Google G Suite,

4) Heroku/Salesforce [link: https://www.salesforce.com/company/privacy/full_privacy/] for servers, databases

Info shared: User information, aggregated information

5) HubSpot [link: https://legal.hubspot.com/privacy-policy] for sending emails on our behalf

Info shared: User information and user activity

6) Intercom [link: https://www.intercom.com/terms-and-policies#privacy] for managing customer service contacts, emails

Info shared: User information, user activity, contact activity, marketing content

7) mLab/MongoDB [link: https://mlab.com/company/legal/privacy/] for data storage

Info shared: User information, visit logs

8) OneSignal [link: https://onesignal.com/privacy_policy] for sending push notifications on our behalf

Info shared: Hashed user identifiers, user-generated content

9) Papertrail [link: https://papertrailapp.com/] for Service logging and fixing errors

Info shared: IP address, browser information

10) Plivo [link: https://www.plivo.com/legal/privacy/] for sending text messages on our behalf

Info shared: telephone number, user-generated content

11) Redis Labs [link: https://redislabs.com/privacy/] for data storage

Info shared: user information, events

12) SendGrid/Twilio [link: https://sendgrid.com/policies/privacy/] for sending emails on our behalf

Info shared: Email address, user information, user-generated content

Product Data List

	DATA Collected for Operation	**General Purpose of Data Collected**
1	STUDENT FIRST AND LAST NAME	Required to support Product Functionality
2	STUDENT ID	Required to support Product Functionality
3	STUDENT GRADE	Required to support Product Functionality
4	STUDENT GENDER	Required to support Product Functionality
5	STUDENT LANGUAGE	Required to support Product Functionality
6	PARENT FIRST AND LAST NAME	Required to support Product Functionality
7	PARENT PHONE/MOBILE NUMBER	Required to support Product Functionality
8	PARENT EMAIL ADDRESS	Required to support Product Functionality
9	SCHOOL NAME	Required to support Product Functionality
10	PHOTOGRAPH,VIDEO OR AUDIO FILE	Required to support Product Functionality
11	Browser Type	Statistics/Customer Service
12	Access Time	Statistics/Customer Service
13	Time spent on Site	Statistics/Customer Service
14	Page Views	Statistics/Customer Service
15	Referring URL	Statistics/Customer Service

Accuracy Statement

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

Signed and agreed:

DocuSigned by:
Jason Olim
D17617F025D14FA...

(Signature)

Jason Olim
CTO
ClassTag, inc.

06/24/2019

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

DocuSigned by:
Amber Lindsay
4936610B3823488...

(Signature)

Amber Lindsay
President & CEO
iKeepSafe

06/24/2019

Copyright