iKeepSafe Product Profile
StudyBee

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

Product Overview

StudyBee makes standards-based grading directly in Google Classrooms possible. By assigning standards to assignments in Google Classroom students can easily see what is expected of them for each assignment, helping them to progress through each level of mastery. This allows teachers to give students relevant formative feedback and track their progress through each area of learning. Using this information, teachers can then differentiate instruction to meet each student needs at the appropriate level of proficiency.

https://studybee.se/?lang=us

Agreement

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

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

Prohibitions:

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

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

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

Obligations:

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

6. StudyBee will delete student information when requested by school district.

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

Children's Online Privacy Protection Act ("COPPA") (15 U.S.C §§ 6501-6506)

1. StudyBee contracts directly with schools and, as such, may rely on consent from the school instead of the parents for collection of personal information from students when data collected is for the use and benefit of the school, and not for any other commercial purposes.

2. StudyBee makes available clearly written policies explaining what data it collects from users, how such data is used, stored and to whom it may be disclosed.

3. StudyBee makes an available copy of the privacy policy available to the school prior to completion of the sale, download or installation of the product.

4. StudyBee provides the school a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information.

5. StudyBee collects limited data from or about children that is reasonably needed to provide users with a feature or activity, or to perform a valid business function that meets the strict definition of support for internal operations.

6. StudyBee does not/will not condition a child's participation in an activity on the child disclosing more personal information than is reasonably necessary to participate in such activity.

7. StudyBee maintains reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. It takes reasonable steps to release children's personal information only to service providers and third parties who can maintain the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

8. StudyBee will retain personal information collected online from a child only as long as is reasonably necessary to fulfill the purpose for which the information was collected. It must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

9. StudyBee will conduct annual training related to data privacy and security, including COPPA requirements, for all employees responsible in whole or in part for design, production, development, operations and marketing of their products. Such training will include all employees who are directly or peripherally involved in collection, use, storage, disclosure or any other handling of data.

10. StudyBee will not make material changes to its privacy and security policies, including adding practices around new or additional data collection, or changes that may lessen the previously noted protections without prior notice to the school, separate from any notice in a "click wrap" agreement. It will notify schools and obtain the prior verifiable consent for any material changes to its privacy policy that affect the collection or use of personal information from students.

Data Review Process

StudyBee provides users direct access to the personally identifiable information that they provide to StudyBee via product functionality. Users also have the ability to contact StudyBee for access to all personal information on file by contacting StudyBee through privacy@studybee.io.

You can ask us for a copy of your personal information or your child's personal information, which we will send to you as soon as possible (but within 30 days). We may require you to provide verification of your identity before providing a copy of the information we hold.

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 privacy@studybee.io .

You can also ask us to delete your account and all the associated personal data held by StudyBee by emailing us at privacy@studybee.io.

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 privacy@studybee.io . If further data collection is stopped, those individuals may no longer be able to use StudyBee.

General inquiries related to privacy may be directed to:

email: privacy@studybee.io,

Phone :46 730247279

StudyBee AB
Djäknegatan 9,
211 35 Malmö,
Sweden

Security Protocols

StudyBee 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

Securing data in transit

Data is vulnerable to unauthorized access as it travels across the Internet or within networks. For this reason, securing data in transit is a high priority for Google. The Google Front End (GFE) servers support strong encryption protocols such as TLS to secure the connections between customer devices and Google's web services and APIs. Cloud customers can take advantage of this encryption for their services running on Google Cloud Platform by using the Google Cloud Load Balancer. The Cloud Platform also offers customers additional transport encryption options, including Google Cloud VPN for establishing IPSec virtual private networks.

Data at Rest:

StudyBee' data storage is provided by Google Cloud.

Encryption methodology is inherent in their data storage systems. And, is replicated in encrypted form for backup and disaster recovery.

Data Center Security:

StudyBee uses Google Cloud Data Centers:

Google cloud servers in Frankfurt Germany for both data and back-up. For U.S customers; Google Cloud servers both for data and back-up are in the USA.

Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a security corridor which implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Less than one percent of Googlers will ever set foot in one of our data centers.

Personnel:

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

Training: Employees of StudyBee will receive annual privacy and security training that includes FERPA, COPPA 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, StudyBee will provide schools with:

[X] audit rights to the school's data

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

Data Breach

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

StudyBee 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

StudyBee states they will not keep your information for longer than we need to for the purposes listed in this policy. We may delete certain personal and usage data if you haven't used your account for more than 2 years.

Research

StudyBee stated; a name and email address is connected to the activities we store in Mixpanel. This is done in order to understand how often a certain activity is done and if there is a need for usability improvement in some parts. The email connected to activities are stored in 3 months, then it is deleted.

Third Parties

StudyBee 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.

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

StudyBee utilizes the following third-party vendors:

Google Cloud
Freshworks
Mixpanel
Tenesys
10-Clouds

Product Data List

Data Collection:

- Student Information: Course Assignment, Grades, Base Assessment, Assessment for each learning objective, Self-assessment for each learning objective, Student profile picture, Student email address
- School Information: School name, address, municipality, email address, organization code, telephone number, Educational level.
- Guardian Information: Name and email address
- Information you share with us, for example in an email, form or support issue.
- Some technical information about how you use StudyBee, for example, the type of device, your operating system or IP address.
- When you sign into StudyBee using a Google account, we will receive your full name and profile picture from your account.

Accuracy Statement

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

Signed and agreed:

DocuSigned by:
73AE77889E8B44C...
(Signature)

Ted Möller
StudyBee
tel: +46 0706999183

03/22/2021

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

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

Amber Lindsay
President & CEO
iKeepSafe

03/22/2021

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.