iKeepSafe Product Profile
TeamBuildr

Introduction

The *iKeepSafe* FERPA,COPPA and CSPC (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 *iKeepSafe* Product Profile is intended to assist you in determining whether TeamBuildr complies with FERPA, COPPA and CSPC (California). It indicates that TeamBuildr has been assessed for alignment with the iKeepSafe FERPA and COPPA Guidelines.

Product Overview

TeamBuildr is an online strength and conditioning and Physical Education software

platform for high schools.

www.teambuildr.com

Agreement

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

1. Student records obtained by TeamBuildr 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 TeamBuildr.

2. TeamBuildr users may retain possession and control of their own generated content.

3. TeamBuildr will not use any information in a student record for any purpose other than those required or specifically permitted by the TeamBuildr 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, TeamBuildr users may access, correct, update, or delete personal information in their profile by signing into TeamBuildr, accessing their TeamBuildr account, and making the appropriate changes.

5. TeamBuildr 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, TeamBuildr will promptly notify users unless specifically directed not to provide such notification by law enforcement officials.

7. TeamBuildr 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. TeamBuildr 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. TeamBuildr prohibits using personally identifiable information in student records to engage in targeted advertising.

10. TeamBuildr 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.

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

1. TeamBuildr 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. TeamBuildr 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. TeamBuildr makes a copy of the privacy policy available to the school prior to completion of the sale, download or installation of the product.

4. TeamBuildr 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. TeamBuildr 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. TeamBuildr 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. TeamBuildr 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. TeamBuildr 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. TeamBuildr 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. TeamBuildr 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. 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.

C. . As related to Student Online Personal Information Protection Act (SB 1177 -"SOPIPA"), TeamBuildr agrees:

Prohibitions:

1. TeamBuildr does not target advertising via its website or on any other website using information about a K-12 student acquired from a use of the technology.

2. TeamBuildr does not use information, including persistent unique identifiers, created or gathered by the site to amass a profile about a K–12 student except in furtherance of K–12 school purposes.

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

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

Obligations:

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

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

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

Data Access and Review Process

A data access request asks TeamBuildr to provide, correct or delete personal information. All data access requests are lodged via an email to privacy@teambuildr.com.

Any party wishing for TeamBuildr to provide or correct their personal information can make a

request either via their school or directly to TeamBuildr and they will provide or correct the information as instructed.

TeamBuildr collects data on behalf of schools. Any party wishing for TeamBuildr to provide, correct or delete their personal information can make a request via their school, and they will fulfill the data request in a timely manner.

Security Protocols

TeamBuildr 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

TeamBuildr Web-based data are transmitted using transport-level security provided by HTTP over SSL connections (HTTPS). Data is always encrypted at rest and in transit. All TeamBuildr production client facing applications requiring SSL certs should be set with a minimum key length of 2048 bits. Public key info RSA 2048-bit Signature algorithm SHA256WITHRSA. This

Data at Rest

TeamBuildr uses encrypted AWS RDS databases. Amazon RDS encrypted DB instances use the industry standard AES-256 encryption algorithm to encrypt data on the server that hosts Amazon RDS DB instances.

Data Center Security

TeamBuildr 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 TeamBuildr will receive annual privacy and security training that includes

FERPA and COPPA.

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, TeamBuildr will provide schools with:

[X] audit rights to the school's data

Data Breach

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

TeamBuildr 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 TeamBuildr.

Data Deletion

TeamBuildr stores your personal information for as long as it is necessary to provide products and Services to you and others. Personal information associated with the user account will be kept until the account is deleted or until we no longer need the data to provide products and services.

TeamBuildr may have to retain some information after your account is closed, to comply with legal obligations, to protect the safety and security of our community or our Service, or to prevent abuse of our Terms. At TeamBuildr, a user may delete their account at any time by contacting their school directly or by contacting TeamBuildr at privacy@teambuildr.com.

Third Parties

TeamBuildr 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.

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

TeamBuildr utilizes the following third-party vendors:

Provider	What do they do for us?
Amazon Web Services (AWS)	AWS hosts all of our databases, web servers, login services, emails sent from our application, and more.
Hubspot	Inbound marketing, sales & customer service.
Intercom	Sales, marketing, and support.
Twilio Sendgrid	Communication: Email, SMS, in-app chat.
Fusion Sport	Athletic management system.
Lumin	Athletic management system.
Kinduct	Athlete data consolidation & visualization.
Edge10 Group	Athletic Performance Analytics.

Product Data List

Data Collection by TeamBuildr include the following:

Category	Examples	Collected
A. Identifiers.	Real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address and email address.	YES
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	Real name, address and telephone number. Some personal information included in this category may overlap with other categories.	YES
C. Protected classification characteristics under California or federal law.	Age (40 years or older) and sex ((including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions)	YES
D. Commercial information.	None.	YES
E. Biometric information.	Sleep, health, or exercise data.	YES
F. Internet or other similar network activity.	Browsing history, search history and information on a consumer’s interaction with a website, application, or advertisement.	YES
H. Sensory data.	None.	YES
K. Inferences drawn from other personal information.	Profile reflecting a person’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.	YES
L. Sensitive Personal Information	Personal information collected and analyzed concerning a person’s health.	YES

Accuracy Statement

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

Signed and agreed:

01/20/2021

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

DocuSigned by:
Amber Lindsay
4936610B3823488...

(Signature)

Amber Lindsay
President & CEO
iKeepSafe

Copyright