iKeepSafe

iKeepSafe Product Profile
SurfWisely DBA Precise Cyber Solutions

Introduction

The *iKeepSafe* COPPA 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 SurfWisely complies with COPPA. It indicates that SurfWisely has been assessed for alignment with the iKeepSafe COPPA Guidelines.

Product Overview

https://portal.surfwisely.com

Innovative CyberSecurity awareness training gamified app using sports to teach students cybersecurity concepts and keep them safe.

Agreement

As related to the , Children's Online Privacy Protection Act ("COPPA") (15 U.S.C §§ 6501- 6506) SurfWisely agrees:

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

4. SurfWisely 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. SurfWisely 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. SurfWisely does not and 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. SurfWisely 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. SurfWisely 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. SurfWisely 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. SurfWisely 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 Access and Review Process

Any party wishing for SurfWisely to provide or correct their personal information can make a request either via their school or directly to SurfWisely and they will provide or correct the information as instructed.

A data access request which asks SurfWisely to provide, correct or delete personal information is logged via an email to info@surfwisely.com. Depending on the nature of the request they may require the requestor to provide information to verify their identity, and/or be an authorized agent of their school.

SurfWisely collects data on behalf of schools. Any party wishing for SurfWisely 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

SurfWisely 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

SurfWisely uses secure socket layer technology (SSL) when a user enters any information anywhere on the Service as a default and this technology enables the encryption of that information during server transmission.

Data at Rest

SurfWisely database is encrypted **at rest**, where they store a user's personal information, which converts all personal information stored in the database to an unintelligible form.

Data Center Security

SurfWisely uses Microsoft Azure and these centers conform to the following:

For data at rest, all data written to the Azure storage platform is encrypted through 256-bit AES encryption and is FIPS 140-2 compliant. Proper key management is essential. By default, Microsoft-managed keys protect your data, and Azure Key Vault helps ensure that encryption keys are properly secured. Azure key management also includes server-side encryption that uses service-managed keys, customer-managed keys in Azure Key Vault, or customer-managed keys on customer-controlled hardware. With client-side encryption, you can manage and store keys on-premises or in another secure location.

For data in transit—data moving between user devices and Microsoft datacenters or within and between the datacenters themselves—Microsoft adheres to IEEE 802.1AE MAC Security Standards, and uses and enables your use of industry-standard encrypted transport protocols, such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec).

Please see more information below in the available link:

https://azure.microsoft.com/en-us/solutions/#security-and-governance

Personnel

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

Training: Employees of Precise Cyber Solutions will receive annual privacy and security training that includes 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, Precise Cyber Solutions will provide schools with:

☒ audit rights to the school’s data

☒ access to the results of Precise Cyber Solutions or its third-party security audit

Data Breach

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

Precise Cyber Solutions 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 the SurfWisely.

Data Deletion

SurfWisely 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.

SurfWisely 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 SurfWisely, a user may delete their account at any time by contacting their school directly or by contacting SurfWisely at info@surfwisely.com.

Research

SurfWisely may use data which has been de-identified and/or aggregated for product development, research, analytics and other purposes, including for the purpose of analyzing, improving, or marketing the Services. On certain occasions, SurfWisely may share this data with business partners to improve their services or offerings. If they disclose information to authorized business partners to conduct research on online education or assist in understanding the usage, viewing, and demographic patterns for certain programs, content, services, promotions, and/or functionality on our Service, such data will be aggregated and, or anonymized to reasonably avoid identification of a specific individual.

Third Parties

SurfWisely 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.

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

SurfWisely utilizes the following third-party vendors:

Third Party	Purpose	Information Shared
Microsoft Azure	Hosting	Student User Data

Product Data List

Data Collection by SurfWisely include the following:

	DATA Collected for Operation	General Purpose of Data Collected
1	STUDENT FIRST and LAST NAME	Required to support Product Functionality
2	STUDENT EMAIL ADDRESS	Required to support Product Functionality
3	OTHER STUDENT ID	Required to support Product Functionality
4	SCHOOL NAME	Required to support Product Functionality
5	Other device/usage analytics	Required to support Product Functionality

Accuracy Statement

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

Signed and agreed:

(Signature)

Myron Grover
Precise Cyber Solutions
P.O. 56 Nolensville, TN 37135
629-888-3083

06/25/2021

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

DocuSigned by:
Amber Lindsay
4936610B3823488...

(Signature)

Amber Lindsay
President & CEO
iKeepSafe

06/25/2021

Copyright