



iKeepSafe Product Profile CYBER.ORG National Cyber Cup

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 CYBER.ORG, specifically the [National Cyber Cup](#), complies with COPPA. It indicates that the [National Cyber Cup](#) has been assessed for alignment with the iKeepSafe COPPA Privacy Program Guidelines.

Product Overview

National Cyber Cup by CYBER.ORG

The National Cyber Cup by CYBER.ORG is a free, jeopardy-style, CTF competition for elementary, middle school and high school students with a focus on cybersecurity themes and challenges. There are two sites associated with NCC: a mobile competition site and a mobile registration site. The NCC platform has 3 different types of users- Coaches (team sponsors), student participants, parents (registration only). There are three divisions: Elementary (4-5), Middle School (6-8), and High School (9-12). Students receive points for answering questions correctly. There is a live scoreboard for students to determine how they are doing compared to other students in their division.

CYBER.ORG

[National Cyber Cup by CYBER.ORG](#)

Agreement

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

1. CYBER.ORG 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.
2. CYBER.ORG makes a copy of the privacy policy available prior to completion of the sale, download or installation of the product.
3. CYBER.ORG provides 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.
4. CYBER.ORG 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.
5. CYBER.ORG 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.
6. CYBER.ORG maintains reasonable procedures to protect the confidentiality, security, and integrity of personal information collected. 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.
7. CYBER.ORG 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 will delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.
8. CYBER.ORG 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.
9. CYBER.ORG 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.

Security Protocols

The following is a general overview of data security protocols of CYBER.ORG

Data in Transit:

All data is transmitted over HTTPS.

Data at Rest:

Data at rest is encrypted using AES 256-bit encryption

Data Center Security:

CYBER.ORG utilizes data centers operated by AWS. Data backups are stored on AWS S3 with secure bucket and AWS encryption. AWS comes with a public and private key authentication to access the cloud server running the platform and storing the data and the data backups.

[https://aws.amazon.comCloud Computing Services - Amazon Web Services \(AWS\)/compliance/iso-27001-faqs/](https://aws.amazon.comCloud%20Computing%20Services%20-%20Amazon%20Web%20Services(AWS)/compliance/iso-27001-faqs/)

<https://aws.amazon.com/compliance/data-privacy-faq/>

Personnel:

Training: CYBER.ORG conducts privacy and security training for all employees.

Access: Access to children's data is limited to those employees who need access to perform job responsibilities. All employees with access to Children's PII have undergone background checks.

Data Deletion

The National Cyber Cup platform stores your Personal Information for as long as it is necessary to provide their services to you. Personal Information associated with the account will be kept until the account is deleted. Please note they may have to retain some information after the 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. A user, of course, can delete the account at any time, as per the "Deleting Your Account" section in the Privacy Policy.

Access to Audit

Once per year, CYBER.ORG will provide parents with:

☒

audit rights to their child's data

☒

access to the results of CYBER.ORG or its third-party security audit

Data Breach

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

CYBER.ORG 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 Review Process

CYBER.ORG provides users direct access to their personally identifiable information that they provide to the National Cyber Cup through product functionality.

Registered Users may access or modify their personal information provided to CYBER.ORG which is associated with the user account at any time. Users can log in to the National Cyber Cup platform and visit their account settings page or email us at apps@cyber.org to exercise their rights at any time.

If the user has registered for a Child Account on the National Cyber Cup platform, the user may view, edit, or delete any of your profile information or your preferences at any time by logging into the National Cyber Cup platform and accessing the account settings page.

General inquiries related to privacy may be directed to:

6300 East Texas St. Bossier City, LA 71111

318- 759-1600

email: apps@cyber.org.

Research

CYBER.ORG stated; We use none of the customer data for research or statistical purposes at this time. If data is used for behavioral or product improvements the data is aggregated and cannot be identified to any particular individual.

CYBER.ORG may also analyze information that does not contain "Personal Information" (or contains "Personal Information" in anonymous or aggregated form) for trends and statistics, such as through the use of Google Analytics or other similar analytics services.

CYBER.ORG does not use end user data in any non-production environments including testing, development and training. CYBER.ORG does not use end user data for production improvement or research unless the data has been de-identified. CYBER.ORG will only access non-aggregated personal information for troubleshooting purposes with direct consent and permission from the parent or guardian.

Third Parties

CYBER.ORG 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.

CYBER.ORG 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. CYBER.ORG has agreements in place with all third parties with access to child 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 CYBER.ORG’ data privacy and security policies and expectations.

Third Party	Purpose	Information Shared
AWS	Hosting service	
Heroku	Hosting service	

Product Data List

DATA Collected	General Purpose of Data Collected
STUDENT FIRST and LAST NAME	Required to support Product Functionality
STUDENT AGE	Required to support Product Functionality
STUDENT ETHNICITY	Possible for grant reporting purposes
STUDENT GENDER	Possible for grant reporting purposes
PARENT FIRST AND LAST NAME	Required to support Product Functionality
PARENT EMAIL ADDRESS	Required to support Product Functionality
SCHOOL/ORGANIZATION	Required to support Product Functionality
Team Sponsor Name	Required to support Product Functionality
LEGAL ADDRESS	Location for prizes to be sent
Other device/usage analytics	Business Analytics

Accuracy Statement

CYBER.ORG hereby confirms the accuracy and truthfulness of all information contained in the CYBER.ORG, specifically the [National Cyber Cup](#) Product profile, and has authorized iKeepSafe to make the profile available to any interested third parties.

Signed and agreed:

Signed by:


CA8097A24F1D49B...

(Signature)

Kevin Nolten, President CIC
6300 East Texas St. Bossier City, LA 71111
318- 759-1600
email: apps@cyber.org.

01/06/2025

CYBER.ORG, specifically the [National Cyber Cup](#) has been reviewed and found in alignment with iKeepSafe's COPPA Privacy Program Guidelines as indicated by this product profile. CYBER.ORG, specifically, the [National Cyber Cup](#) has been awarded the iKeepSafe COPPA Privacy Program badge.

DocuSigned by:

4936610B3823488...

(Signature)

Amber Lindsay
President & CEO
iKeepSafe

01/06/2025

Copyright

© 2020 Internet Keep Safe Coalition (iKeepSafe). All rights reserved. iKeepSafe's California Privacy Assessment Program™ materials have been developed, copyrighted, and distributed for incidental, classroom use only. iKeepSafe's copyright notice and distribution restrictions must be included on all reproductions whether in electronic or hard copy form. These materials are intended to convey general information only and not to provide legal advice or any other type of professional opinion.