iKeepSafe

iKeepSafe Product Profile
NextUp

Introduction

The iKeepSafe FERPA 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 NextUp complies with FERPA. It indicates that NextUp has been assessed for alignment with the iKeepSafe FERPA Guidelines.

Product Overview

www.transitioncurriculum.com

www.nextup.work

NextUp is a comprehensive transition curriculum consisting of weekly lesson videos, lesson plans, supplemental activities, assessments, and more. NextUp equips teachers with the tools and resources to enhance student post-secondary success in employment, education, and independent living.

Agreement

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

1. Student records obtained by NextUp 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 NextUp.

2. NextUp users retain possession and control of their own generated content by contacting the educational institution.

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

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

    Notification shall identify:

    (i) the date and nature of the unauthorized use or disclosure;
    (ii) the Private Data used or disclosed;
    (iii) general description of what occurred including who made the unauthorized use or received the unauthorized disclosure;
    (iv) what NextUp has done or shall do to mitigate any effect of the unauthorized use or disclosure;
    (v) what corrective action NextUp has taken or shall take to prevent future similar unauthorized use or disclosure; and
    (vi) who at NextUp the User can contact. NextUp will keep the User fully informed until the incident is resolved.

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

10. NextUp will not make material changes to our Terms of Service 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 Access and Review Process

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

A data access request which asks NextUp to provide, correct or delete personal information is lodged via an email to NextUp@TransitionCurriculum.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.

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

NextUp 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

NextUp 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

NextUp's 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

NextUp uses AWS and they conform to the following:

AWS adheres to the following privacy standards:

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 NextUp 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, NextUp will provide schools with:

[X] audit rights to the school's data

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

Data Breach

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

NextUp 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 NextUp.

Data Deletion

NextUp 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.

NextUp 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 NextUp, a user may delete their account at any time by contacting their school directly or by contacting NextUp at NextUp@TransitionCurriculum.com.

Research

NextUp 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, NextUp 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

NextUp 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.

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

NextUp utilizes the following third-party vendors:

Third Party	Purpose	Information Shared
Heroku	Hosting	All Database Tables
Mixpanel	Event Tracking	Account level event tracking
Amplitude	Event Tracking	Account level event tracking
accessiBe	Accessibility Enhancements	Cookies for saving preferences
Youtube	Hosting Videos	None
Vimeo	Hosting Videos	None
Zoom	Webinar/Training conference tools	emails of those who sign up

Product Data List

Data Collection by NextUp include the following:

#	Data	Purpose Of Transfer Or Share
1	Student First And Last Name	First Name collected to allow students to have different tasks assigned in business
2	School Name	Account Management
3	Geolocation Data	Collected by Mixpanel for platform analysis
4	Photograph, Video Or Audio File	Allow students or teachers to upload pictures of items being sold in business

5	Browser Type	Collected by Mixpanel for platform analysis
6	Page Views	Collected by Mixpanel for platform analysis
7	Others (Business Logo)	Account Management
8	Others (Business Name)	Account Management
9	Others (Establishment)	Account Management
10	Others (Teachers Email)	Account Management
11	Others (Teacher Password)	Account Management
12	Others (School District Name)	Account Management
13	Others (Teacher Name)	Account Management

Accuracy Statement

NextUp hereby confirms the accuracy and truthfulness of all information provided to iKeepSafe during the assessment process. NextUp hereby confirms the accuracy and truthfulness of all information contained in the NextUp profile and has authorized iKeepSafe to make the profile available to any interested schools.

Signed and agreed:

Chad Logsdon
(Signature)

Chad Logsdon
Lead Product Engineer
Transition Curriculum Inc. DBA NextUp
311 E. Main Street, Suite 512
Galesburg, Illinois 61401 Email Address:
nextup@transitioncurriculum.com Phone Number:
309-790-3727

02/03/2025

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

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

Amber Lindsay
President & CEO
iKeepSafe

02/03/2025

Copyright