iKeepSafe Product Profile
Wakelet

Introduction

The iKeepSafe 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 *iKeepProfile* is intended to assist you in determining whether Wakelet complies with COPPA, FERPA, SOPIPA, California AB 1584, and other California state laws and district policies. It indicates that Wakelet has been assessed for alignment with the iKeepSafe California Privacy Program Guidelines.

Product Overview

Wakelet: https://Wakelet.com

Wakelet is a free content curation platform that allows users to save, organize and share content
from across the web.

Wakelet is the easiest way to capture, organize and share multimedia resources with Students, Teacher and the learning community.

Agreement

A. As related to the Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. Section 1232g) and California AB 1584 (Buchanan) Privacy of Pupil Records: 3rd-Party Digital Storage & Education Software (Education Code section 49073.1), Wakelet agrees:

1. Pupil records obtained by Wakelet from an LEA or School continue to be the property of and under control of that Educational Representative. Wakelet does not directly touch any information nor have routine access to the data and recognizes that any information exchanged is the property of the School.

2. It shall not use any information in a pupil record for any purpose other than those required or specifically permitted by the Wakelet Terms of Service and Privacy Policy.

3. Parents, legal guardians, or eligible pupils may review personally identifiable information in the pupil's records and correct erroneous information by contacting their School.

4. It is committed to maintaining the security and confidentiality of pupil records. To that end, Wakelet has taken the following actions: (a) limiting employee access to student data based on roles and responsibilities; (b) conducting background checks on employees who have access to student data; (c) conducting privacy training that includes FERPA for employees with access to pupil data; (d) protecting personal information with technical, contractual, administrative, and physical security safeguards in order to protect it from unauthorized access, release or use.

5. It will delete personally identifiable data upon request of the Educational Representative and/or upon expiration of the services agreement. See Security Protocol section.

6. It agrees to work with the School 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 pupil records and to correct any inaccuracies therein as described in statement 4 above.

7. It prohibits use of personally identifiable information in pupil records to engage in targeted advertising.

8. It 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 Schools, separate from any notice in a “click wrap” agreement.

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

Prohibitions:

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

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

Obligations:

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

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

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

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

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

Security Protocols

The following is a general overview of data security protocols of Wakelet:

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:

Wakelet utilizes data centers operated by AWS who have extensive experience in designing, constructing, and operating large-scale data centers.

AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, and 27018:2014.

ISO/IEC 27001:2013 Compliance - Amazon Web Services

AWS aligns with the CSA STAR Attestation and Certification based on the determinations in our third-party audits for System and Organization Controls (SOC) 2 Reports and ISO 27001:

CSA - Amazon Web Services

Personnel:

Training: Wakelet conducts privacy and security training for all employees.

Access: Access to student data is limited to those employees who need access to perform job responsibilities. All employees with access to PII/PHI have undergone background checks.

Data Deletion

Wakelet stores the information they collect only for as long as necessary to fulfil the purposes they collected it for, including for the purposes of satisfying any legal, accounting or reporting requirements.

Wakelet stores the information they collect from Registered Users for as long as the user has an Account and for 14 days thereafter. After this time, it will be purged from their data store and caches. Logs may contain some user information and are retained for up to 30 days. The incremental back-up system of the AWS Dynamo data store can roll back tables over a time period of up to 35 days. Therefore, data is completely erased after 49 days. Anonymous aggregated analytic data is held in Google Analytics indefinitely.

Wakelet stores the information they collect from Users (without a Wakelet account) for 30 days, until logs are cleared. Anonymous aggregated analytic data is held in Google Analytics indefinitely.

Wakelet periodically cleanse all information stored and will delete your IP address 30 days after collection.

Access to Audit

Once per year, Wakelet will provide schools with:

[X] audit rights to the school's data

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

Data Breach

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

Wakelet 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

Wakelet provides users direct access to the personally identifiable information that they provide to Wakelet via product functionality.

Registered Users may access or modify their personal information provided to Wakelet which is associated with the user account at any time. Users can log in to Wakelet and visit their account settings page or email us at admin@wakelet.com to exercise their rights at any time.

Wakelet cannot delete your personal information without deleting the registered user account. Wakelet may not accommodate a request to change information if they believe

the change would violate any law or legal requirement or cause the information to be incorrect.

Wakelet wants all users to be in control of your information and they provide their registered users with certain tools in the account settings page.

General inquiries related to privacy may be directed to:

Wakelet Limited
Manchester Technology Centre
Oxford Road
Manchester
M1 7ED
United Kingdom

Third Parties

Wakelet 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.

Wakelet 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. Wakelet 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 Wakelets' data privacy and security policies and expectations.

Your California Privacy Rights: California Civil Code Section 1798.83-1798.84 permits users that are California residents to request certain information regarding our disclosure of personal information to third parties for such third parties' direct marketing purposes. If you are a California resident and would like to make such a request, please contact us at support@wakelet.com

Wakelet utilizes the following third-party vendors:

Provider	How Wakelet uses the Provider	What information we share

AWS (Privacy Policy)	Holds our main data store and hosts our Website and underlying infrastructure.	All personal information, including uploaded content and request data is stored on AWS. All information is encrypted at rest.
Cloudinary (Privacy Policy)	Hosting for some of our image content	Uploaded images may be sent to Cloudinary, but there is no direct association to a user account
Mixpanel (Privacy Policy)	Enables us to continue improving the Services based on trends observed in behaviours	Aggregated user behaviour, such as pages visited, and features used on the site
FullStory (Privacy Policy)	Enables us to continue improving the Services based on trends observed in behaviours	Pseudonymised user behaviour recordings, such as pages visited, and features used on the site. Not enabled for users in the EU.
Mailchimp (Privacy Policy)	Sending out newsletters and other content via email	Email subscriptions, including email addresses and summarised public Wakelet information
Azure (Privacy Policy)	Adult content detection	Uploaded images may be sent to Azure, but there is no direct association to a user account
SendGrid (Privacy Policy)	Sending out email notifications	Email addresses, names and some information required to populate the notifications, such as images and collection titles
Embed.ly (Privacy Policy)	Providing some supplemental information about entered links	Some URLs entered into the site, but no association with accounts

Tawk (Privacy Policy)	Is used to manage support issues, and live support chat	Email addresses, provided names and social media handles of users contacting our support channel as well as the content of the messages
Zendesk (Privacy Policy)	Is used to manage support issues	Email addresses, provided names and social media handles of users contacting our support channel as well as the content of the messages
Google Analytics (Privacy Policy)	Enables us to continue improving the Services based on trends observed in behaviours	Aggregated user behaviour, such as pages visited, and features used on the site
Pushwoosh (Privacy Policy)	Is used to push notifications to mobile clients	Receives the content of push notification messages, as well as a device identifier
Unbounce (Privacy Policy)	Used to host a number of static pages	IP address
Slack (Privacy Policy)	Is used for team messaging	May include information necessary to handle support requests such as a username, real name or email address. Any content older than 30 days is automatically removed.
Loggly (Privacy Policy)	Centralised error logging and log management in order to help us diagnose and detect problems in the product	Raw log data and IP addresses.

Product Data List

Data Collection by Wakelet:

#	Data Collected for Operation	General Purpose of Data Collection
1	Student First and Last Name	Required to support product functionality
2	Student Email Address	Required to support product functionality
3	Student Password	Required to support product functionality
4	Student DOB/Age	Required to support product functionality
5	School Name	To support internal operations
6	School Address	To support internal operations
7	Geolocation	Required to support product functionality
8	Teams, Clubs, Hobbies	Required to support product functionality
9	Photograph, Video or Audio File	Required to support product functionality
10	Browser Type	Analytics
11	Access time	Analytics
12	UDID	Analytics
13	TIME SPENT ON SITE	Analytics
14	PAGE VIEWS	Analytics
15	REFERRING URLS	Analytics
17	Search Activity	Required to support product functionality - not collected for U13 users.
18	Uploaded Documents	Required to support product functionality
19	Contents of private chat messages	Required to support product functionality

Accuracy Statement

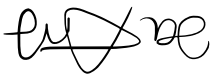
Wakelet. hereby confirms the accuracy and truthfulness of all information contained in the Wakelet Product profile, and has authorized iKeepSafe to make the profile available to any interested schools.

Signed and agreed:

Jamil Khalil, CEO
Wakelet
Bright Building
Manchester Science Park
5 Pencroft Way
Manchester
M15 6GZ
United Kingdom

Jamil Khalil
(Printed Name)

Founder & CEO
(Title)



(Signature)

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

DocuSigned by:
Amber Lindsay
4936610B3823488...

(Signature)

Amber Lindsay
President & CEO iKeepSafe

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.