iKeepSafe Product Profile
Gradient Learning and CZI
Along

Introduction

The *iKeepSafe* FERPA and 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 Along offered by Gradient Learning, with support from the Chan Zuckerberg Initiative ("**CZI**") (collectively, "**Along**") complies with FERPA and COPPA. It indicates that Along has been assessed for alignment with the iKeepSafe FERPA and COPPA Guidelines.

Product Overview

Along is a free, web-based, digital teacher-student connection builder - helping teachers to better understand their students and increase student engagement in the classroom. The Services enabled by Along have been developed to facilitate meaningful communication (in the form of multiple choice questions, asynchronous text, video and/or other supported methods of communication) between teachers and students through research-informed reflection questions and resources.

Along.org

Agreement

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

1. Student records obtained by Along 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 Along.

2. Along users retain possession and control of their own original content that they submit to Along.

3. Along will not use any information in a student record for any purpose other than those required or specifically permitted by the Along User Agreement 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 or teacher. Additionally, Along users may access personal information in their profile by signing into their Along account. To correct, update, or delete personal information in their profile, Along users should reach out to the Along help center to make the appropriate changes.

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

7. Along 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. Along agrees to work with educational institutions to ensure compliance with FERPA and 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. Along prohibits using personally identifiable information in student records to engage in targeted advertising.

10. Along will not make material changes to the Along User Agreement 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. Along contracts directly **with schools** through the **teachers** 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 for educational purposes only.

2. Along 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. Along makes a copy of the privacy policy available to the **teacher/school** prior to completion of the account setup.

4. Along provides the **teacher/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. Along collects limited data from or about children that is reasonably needed to provide users with a feature or activity, or to perform a business activity that meets the definition of "support for internal operations" under COPPA.

6. Along 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. Along 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. Along 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. Along will conduct annual training related to data privacy and security, including FERPA and COPPA requirements, for all employees responsible in whole or in part for the 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. Along 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. Along 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

Along collects data on behalf of schools. Any party wishing for Along to provide or correct their personal information can make a request either via their school or directly to Along and as legally permitted, Along will provide or correct the information as instructed and in a timely manner.

A data access request which asks Along to provide, correct or delete personal information is lodged via an email to privacy@along.org or through the help center. Depending on the nature of the request, Along may require the requestor to provide information to verify their identity, and/or be an authorized agent of their school.

Security Protocols

Along 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

Access to the Along service occurs via encrypted connections (HTTP over TLS, also known as HTTPS) which encrypt all data before it leaves Along's servers and protects that data as it transits over the internet. We use HTTP Strict Transport Security to ensure that pages are loaded over HTTPS connections and our TLS configuration receives an A+ from Qualys SSL Labs.

Data at Rest

All personally identifiable information is encrypted at rest using modern encryption algorithms such as AES--256 or stronger.

Data Center Security

Along 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 the housed data.

Please see more information below in the available link:

Amazon Web Services (AWS)   https://aws.amazon.com/security/

Personnel

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

<u>Training</u>: Employees of Gradient Learning receive annual privacy and security training that includes information about FERPA and COPPA.

<u>Access</u>: Access to student data is role-based; limited to those employees who need access to perform job responsibilities.

Access to Audit

Once per year, Gradient Learning and CZI will provide schools with:

☐   audit rights to the **school's data**

☒   access to the results of Gradient Learning and CZI, or its **third-party security audit**

Data Breach

In the event of an unauthorized disclosure of a student's records, Along will promptly notify the school without undue delay or as required by the applicable law. Notification shall identify:

a. the name and contact information of the reporting school subject to Along's Security Incident Notification section in its User Agreement;

b. a list of the types of personally identifiable information that were or are reasonably believed to have been the subject of a security incident;

c. if the information is known at the time the security incident notification is provided, then either (1) the date of the security incident, (2) the estimated date of the security incident, or (3) the date range within which the security incident occurred. The security incident notification shall also include the date of the notice;

d. whether, to the knowledge of Along at the time notice is provided, the notification was delayed as a result of a law enforcement investigation or request; and

e. a general description of the security incident, if that information is possible to determine at the time the notice is provided.

Data Deletion

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

Along may have to retain some information after your account is closed, to comply with legal obligations, to protect the safety and security of the community or Along, or to prevent abuse of Along's terms in the User Agreement.   A user may delete their account at any time by contacting their school directly or by contacting Along via Help Center or at privacy@along.org.

Research

Along 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 Along. On certain occasions, Along may share this data with service providers to support the operation of the Services, such as through document management, data hosting, and provisioning customer service tools related to Along. Along will only share de-identified information should Along wish to demonstrate how Along is used, its efficacy, or otherwise provide information or marketing materials related to Along. Along may share aggregated and/or non-personally identifiable information publicly (such as statistics about visitors, and website traffic patterns).

Third Parties

Along does not sell, trade, lease or loan the personal information it collects or maintains, in the course of providing the service, to any third party for any reason, including direct marketers, advertisers, or data brokers.

Along 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. Along have 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 Along's data privacy and security policies and expectations.

Along utilizes the following third-party vendors:

Technical Service Providers

Name of Service Provider with Link to Privacy Policy	Service	Details
Amazon Web Services (AWS)	Hosts databases and servers that power and backup Along; also provides email service and analytics support.	We store the full Along content and traffic data on AWS servers (all personal information written to disk is encrypted). We use Amazon Simple Email Service to send emails to users and provide analytics.
Appcues	Augments the user experience in easily customizable ways to better support user onboarding and feature adoption.	Appcues triggers customizable experiences in the UI based on non-personally identifiable information such as prior usage of specific features (e.g. show a reminder if a user hasn't yet sent a reflection).
Atlassian	Used to serve https://comealong.statuspage.io/ to notify users about the service outages.	Atlassian will receive the IP address and traffic data of any visitors to the status page. Visitors who choose to subscribe to updates via email or text.

Automattic	Hosts the public website (www.along.org) on the wpvip.com enterprise agile content platform.	Automattic will receive the IP address and traffic data of any visitors to the Along public website.
Chan Zuckerberg Initiative (CZI)	Provides software engineering, technical, and operational support for Along.	Authorized CZI staff have access to the full Along content and traffic data in the course of providing engineering, technical, and operational support to the Along.
Calendly	Online appointment scheduling with members of our technical support and school and teacher success teams.	Calendly is a calendar add-on that receives user emails when users sign up for appointments.
Datadog	Provides monitoring for reliability and performance of the Along service and infrastructure.	Datadog monitors errors and resource usage. No personally identifiable information is transmitted to Datadog.
Databricks	Serves as a data warehouse that powers Along.	The full Along content and off-platform data collected from schools is stored on Databricks' servers (data is always encrypted).
Fivetran	ELT tool for ingesting data from third party platforms into a warehouse.	Fivetran is used for piping email campaign data from Mailchimp into Snowflake and receives the same information as Mailchimp.

Google	Used to understand the effectiveness of the Along marketing site.	Google Analytics and Google Optimize are used to compare visitors on the marketing site and let educators know about Along. These services do not collect personally identifiable information about visitors, including student visitors to the websites.
Google Tag Manager	Used to dynamically trigger firing of tags without code changes.	Google Tag Manager receives data in standard HTTP request logs, all of which is deleted within 14 days of being received. Google Tag Manager does not collect, retain, or share any information about visitors, including student visitors to the websites.
G Suite for Education (Google)	Provides single-sign-on (SSO) authentication for Along users.	For SSO, Google sends Along authentication tokens, email addresses, and name, but not account passwords. Along does not share any information back with Google for this service.
MaestroQA	Enables customer support for Along to evaluate the quality of their responses to requests from users (e.g. students and educators).	Through Zendesk, MaestroQA receives the email addresses of individuals submitting requests, the content of the requests itself (e.g. bug reports, any other help center request, and data pull requests from educators and schools), including attachments.

Mailchimp	Email service for sending emails to educators, school officials, and everyone who requests to receive information from us.	Mailchimp receives names and email addresses of email recipients and the content of the emails, and provides analytics.
Microsoft Office 365 (Azure AD Seamless Single Sign-On)	Provides single-sign-on (SSO) authentication for Along users.	For SSO, Microsoft sends Along an authentication token, email addresses, and name, but not account passwords. Along does not share any information back with Microsoft for this service.
OneTrust	Used to manage cookie consent for the public website (www.along.org).	OneTrust receives the IP address of the visitor to the website and stores the user's preferences in a cookie on their local device. For known students who have previously logged into the Along application on the same device, OneTrust is not loaded and receives no information because all non-essential tracking is turned off and cannot be turned on.
OpenAI	Used to help teachers semantically search for questions in the Along Library.	OpenAI's embedding model powers search for teachers to find relevant resources and questions in the Teacher's Library.

Periscope	Runs various data reports on data previously captured in Along, uploaded data, and data from third party integrations so we can improve the tool.	Periscope has access to the full Along content and traffic data in our data warehouse (Snowflake) in order to run data reports. All connections between Periscope and Snowflake are encrypted.
Salesforce	Houses and tracks partnership agreements, points of contact and other coordination information.	Salesforce receives the names, email addresses, physical addresses and phone numbers of school and district officials, as well as active and prospective Along users (educators only, not students).
Segment	Tool for standardizing data collection for analytics.	Segment receives event data based on user actions taken on Along.
Split	Used to group users into different experiences for feature deployment and verification.	Split is used to track which type of experience(s) the Along application should use and to provide data analysis based on non-personally identifiable information of user events.
SurveyMonkey	Create and send surveys for educators and students, with the intent of improving Along through teacher and student feedback.	SurveyMonkey receives the email addresses of educators and students submitting feedback, the content of the survey feedback requests (e.g. improvements, feature requests and suggestions etc.), and the responses provided.

Wistia	Hosts videos on the public website and help center.	Wistia receives IP address and video usage data for the public videos explaining what Along is and how it works.
Zendesk	Enables customer support for Along in response to requests and supports management of Help Center content.	Zendesk receives the email addresses of individuals submitting requests, the content of the requests itself (e.g. bug reports, any other help center or support request, and any response sent back.

Product Data List
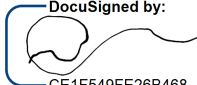
Student data collection by Along includes the following:

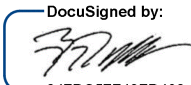|	DATA Collected for Operation	General Purpose of Data Collected
1	STUDENT FIRST and LAST NAME	Required to support Product Functionality
2	STUDENT EMAIL ADDRESS	Required to support Product Functionality
3	PHOTOGRAPH, VIDEO OR AUDIO FILE	Required to support Product Functionality
4	BROWSER TYPE	Business Analytics
5	ACCESS TIME	Business Analytics
6	OTHER PERSISTENT IDENTIFIER	Business Analytics
7	TIME SPENT ON SITE	Business Analytics
8	PAGE VIEWS	Business Analytics
9	REFERRING URLS	Business Analytics

Accuracy Statement

Along 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 teachers/schools.

Signed and agreed:

_____Date: 8/6/2024
(Signature)

Monica Milligan
Executive Director
Gradient Learning

_____Date: 8/9/2024
(Signature)

Brian Manca
VP Finance
CZI

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

_____Date: 8/9/2024
(Signature)

Amber Lindsay
President & CEO
iKeepSafe

Copyright

Copyright