iKeepSafe

iKeepSafe Product Profile
ManagedMethods

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 the ManagedMethods complies with COPPA, FERPA, SOPIPA, California AB 1584, and other California state laws and district policies. It indicates that ManagedMethods has been assessed for alignment with the iKeepSafe FERPA, COPPA and California Privacy Program Guidelines.

Product Overview

ManagedMethods:

https://managedmethods.com

Cloud Application Security – sometimes referred to in the industry as a Cloud Access Security Broker, or CASB – is designed to provide a strong level of visibility, control and protection of various types of cloud applications and the data associated with them.

Cloud application security is a fundamental control layer of cybersecurity. It's primarily concerned with analyzing and controlling what is happening with the school's cloud applications like Google G Suite, Google Drive, Office 365 Mail, OneDrive, SharePoint, Slack, Box, Dropbox and ShareFile.

Agreement

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

1. Student records obtained by ManagedMethods 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 ManagedMethods.
2. ManagedMethods users may retain possession and control of their own generated content.
3. ManagedMethods will not use any information in a student record for any purpose other than those required or specifically permitted by the ManagedMethods Terms and Conditions 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, ManagedMethods users may access, correct, update, or delete personal information in their profile by signing into ManagedMethods, accessing their ManagedMethods account, and making the appropriate changes.
5. ManagedMethods 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, ManagedMethods will promptly notify users unless specifically directed not to provide such notification by law enforcement officials.
7. ManagedMethods 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. ManagedMethods 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. ManagedMethods prohibits using personally identifiable information in student records to engage in targeted advertising.
10. ManagedMethods will not make material changes to our Terms of Use or Privacy Policy, including making significant changes impacting the collection, use, disclosure or retention of data collected without prior notice to the educational user.

As related to the Student Online Personal Information Protection Act (SB 1177 -"SOPIPA"), ManagedMethods agrees:

Prohibitions:

1. ManagedMethods does not target advertising via the ManagedMethods service or on any other website using information about a K-12 student, their families/guardians or educators acquired from a use of the technology.

2. ManagedMethods does not use information, including persistent unique identifiers, created or gathered by the ManagedMethods service to amass a profile about a K–12 student, their families/guardians or educators except in furtherance of K–12 school purposes.

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

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

Obligations:

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

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

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

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

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

ManagedMethods provides users direct access to the personally identifiable information that they provide to ManagedMethods via product functionality. Users also have the ability to contact ManagedMethods for access to all personal information on file by contacting ManagedMethods through support@managedmethods.com

Added to TOS: 6.6 ManagedMethods welcomes your comments and questions regarding this Privacy Policy and we will respond to any request for access to personal information within 30 days. If you believe that ManagedMethods has not adhered to this Privacy Policy, please contact us electronically or via postal mail at the address provided below, and we will use commercially reasonable efforts to promptly determine and remedy the problem. Email: support@managedmethods.com

General inquiries related to privacy may be directed to:

ManagedMethods, INC
719 Walnut Street
Boulder, CO 80302

Email support: support@managedmethods.com
Phone support: (303) 415-3640 option 2
8:00 am-5:00 pm US-Mountain Time

Security Protocols

ManagedMethods 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:

Data is transferred using HTTPS.

Securing data in transit

Data is vulnerable to unauthorized access as it travels across the Internet or within networks. For this reason, securing data in transit is a high priority for Google. The Google Front End (GFE) servers support strong encryption protocols such as TLS to secure the connections between customer devices and Google's web services and APIs. Cloud customers can take advantage of this encryption for their services running on Google Cloud Platform by using the Google Cloud Load Balancer. The Cloud Platform also offers customers additional transport encryption options, including Google Cloud VPN for establishing IPSec virtual private networks.

Data at Rest:

ManagedMethods' data storage is provided by Google Cloud. Encryption methodology is inherent in their data storage systems. And, is replicated in encrypted form for backup and disaster recovery.

Data Center Security:

ManagedMethods uses Google Cloud Data Centers:

Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a security corridor which implements multi-factor access control using security badges and biometrics. Only approved employees with specific roles may enter. Less than one percent of Googlers will ever set foot in one of our data centers.

Personnel:

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

Training: Employees of ManagedMethods 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.

Employees are given access to the minimum services that are required for their job function.

Access to Audit

Once per year, ManagedMethods will provide schools with:

[X] audit rights to the school's data

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

Data Breach

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

ManagedMethods 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,

See: https://managedmethods.com/managedmethods-internal-data-breach-protocol/

Data Deletion

ManagedMethods states they delete the instances and all the data related to the customer upon request. Additionally, they retain the metadata and risks found in a customer environment for up to 3 months. They delete data after this period (3 months) and for discontinued customers, they destroy the data immediately upon deactivation

Research

ManagedMethods stated; We use none of the customer data for research or statistical purposes at this time.

Noted from TOS:

ManagedMethods collects and stores information to monitor and maintain the ManagedMethods Service to you. Such information includes system health and availability, CPU and disk utilization over time, etc. The sole purpose of collecting this data is to monitor the availability of your service and to respond to failures in order to restore the service. ManagedMethods also aggregates anonymized user data, including document and user meta-data, usage and volume statistical information, and other statistics (but not contact information) from our visitors and Users and may provide such anonymous aggregated information to third parties.

Third Parties

ManagedMethods 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.

ManagedMethods 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. ManagedMethods 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 ManagedMethods' data privacy and security policies and expectations.

ManagedMethods utilizes the following third-party vendors:

Google Cloud	Hosting Provider
ZenDesk	Support Ticket System

Product Data List

Data Collection: This was added and/or modified to the TOS/PP section:

Registered Account Information from School/Educators (Name, Address, Billing information, etc.) and Student Information that may be visible during Customer Support/Troubleshooting, including student name, student Email address, file names, creation dates of files, login dates/times and third- party applications students use.

Portions of the Managed Method Service and the Website contain functions for collecting personal information including names and email addresses as well as an individual's or account's access history. We may also collect and track other personally identifiable and non-personally identifiable information about you, such as: your IP address, the type of browser you use, and the website you visited before visiting our Website or ManagedMethods Services.

If you are using the service as an Educational Institution, Student information may be visible during Customer Support and/or Troubleshooting. Personally identifiable information such as Student Name, Student Email Address, file names, creation dates of files, login dates and times, and third-party applications which students use could be viewed on our service by Product Support Staff.

If you register to use the ManagedMethods Service or express interest in obtaining additional information, we require you to give us your contact information, such as your name, company name, address, and email address. We may also ask for additional personal information, such as title, phone number, department name or additional company information, such as annual revenues, number of

employees, or industry. You can opt out of providing this additional information by not entering it when asked.

Accuracy Statement

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

Signed and agreed:

DocuSigned by:
Warren Frebel
3713E6E0664A4AC...
(Signature)

Warren Frebel | VP of Business Development
ManagedMethods
(C) 303.859.0168

02/06/2020

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

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

Amber Lindsay
President & CEO
iKeepSafe

02/06/2020

Copyright

Disclaimer

[1] 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.