



## Securly Inc.

### *Privacy, Safety, and Security Overview*

#### iKeepSafe Privacy Overview

iKeepSafe's privacy assessments review technology services that gather information from children or students. Written policies are reviewed for compliance with relevant data privacy laws. Data governance practices, safety measures, and security practices are examined for alignment with both internal policies and applicable regulation.

#### Securly for Schools Overview

- iKeepSafe appreciates the efforts of educators and others in supporting the responsible use of student data in technology within the classroom.
- iKeepSafe offers an in-depth assessment of edtech vendor practices as it relates to the collection, use, disclosure and security practices regarding student data.
- iKeepSafe has evaluated **Securly** for adherence to the iKeepSafe California Privacy Program guidelines.

#### Product Overview

Securly, Inc. provides cloud-based filtering and monitoring solutions for K-12 educational institutions, Securly for Schools, offering in-school and take-home filtering solutions for students.

Securly audits student posts on Facebook, Twitter and Google+ employing natural language processing algorithms to flag activity on these networks that might be indicative of cyber bullying or self-harm. Securly's algorithms determine the underlying sentiments and emotions behind student's online comments. Algorithms are proprietary information.

#### iKeepSafe Response to CSM Areas of Concern

Securly was noted to have 3 areas of concern by the Common Sense Media Edtech Privacy Evaluation Platform. This document serves to provide additional detail of practices in those areas.

#### Privacy

Securly, as a filtering and monitoring solution, collects a large amount of PII which is stated in their privacy policy. As such, Securly has put in place sound data security and deletion practices as indicated herein. Additionally, the educational institution maintains ownership and control of the data.

## Security

Securly, Inc. maintains a comprehensive set of security practices that are reasonably designed in accordance with commercial best practices

Encryption: Data is encrypted using 256 bit Advanced Encryption Standard (AES). Data is transmitted via HTTPS.

Data Storage: Data is stored in Securly's secure Amazon Web Services (AWS) environment. Database backups are also stored on AWS. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. AWS only provides data center access and information to employees and contractors who have a legitimate business need.

Personnel/Access: Securly conducts annual training/review of FERPA, SOPIPA as well as their company privacy and security policies and access to student data is limited to the cloud-operations engineering personnel. Employees with access to student data have undergone background checks.

Audits: Securly conducts regular audits and provides educational institutions with access to the results on an annual basis.

Data Deletion: Securly deletes personally identifiable data upon request of the LEA and/or upon expiration of the services agreement. All data is deleted within 60-days of expiration of services agreement.

Additionally, Securly obtains a list from the school once a year indicating those student who are no longer enrolled and deletes their information accordingly. This practice aligns with California Education Code § 49073: Collection of Student Information from Social Media.

## Compliance:

Securly for Schools collects and retains student generated content under contractual agreement with an educational institution as part of the filtering and monitoring service, but does not operate a platform by which students create content.



# *iKeepProfile* Securly, Inc. Cloud-based Web Filtering for Schools

## 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 or not Securly, Inc.'s Cloud-based Web Filtering for Schools complies with FERPA, SOPIPA, California AB 1584, and other California state laws and district policies. It indicates that Securly's Cloud-based Web Filtering for Schools has been assessed for and found in alignment with the iKeepSafe California Privacy Program Guidelines. Securly, Inc.'s Cloud-based Web Filtering for Schools has therefore been awarded the iKeepSafe California Program badge.

The *iKeepProfile* is not legal guidance, nor does it guarantee or otherwise assure compliance with any federal or state laws. If you have questions on how to use the *iKeepProfile* to support your school's compliance efforts, please contact your school attorney.<sup>1</sup>

## Product Overview

---

Securly Inc.: - <http://www.securly.com/>

### **Securly for Schools**

Securly, Inc. provides cloud-based filtering and monitoring solutions for K-12 educational institutions offering in-school and take-home filtering solutions for students.

#### Cloud-based Web filtering

Securly's cloud-based web filtering includes:

- Zero-touch filtering of 1:1 take home Chromebooks using a Chrome extension that takes seconds to deploy.
- Support for any heterogeneous mix of 1:1 devices including iPads, Windows, Mac, and Android/Nexus tablets.
- Location based policies for 1:1 devices when off school premises.

Securly filters across categories that matter most to schools while supporting exceptions at both the per-policy level and globally. Additionally, admins have the option of blocking all but a handful of sites for students who are considered at risk.

#### Social Monitoring

Securly audits student posts on Facebook, Twitter and Google+ employing natural language processing algorithms to flag activity on these networks that might be indicative of cyber bullying or self-harm. Securly's algorithms determine the underlying sentiments and emotions behind student's online comments.

## Compliance

---

As a participant in the iKeepSafe California Privacy Program, Securly, Inc. agrees:

### **A. Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. Section 1232g)**

1. **It will act as a School Official as defined by FERPA.** As such, it is under the direct control of the applicable school with regard to use and maintenance of education records.
2. **Education records continue to be the property of and under the control of the school district;** and Securly, Inc. is willing to stipulate as such in a contract or terms of use with the school district.
3. **It collects and retains student generated content as part of the filtering and monitoring service, but does not operate a platform by which students create content** and, as such, the requirement of students retaining possession and **control** of such content does not apply.
4. **It will use education records only for the purposes authorized by the school,** and will not disclose personally identifiable information from education records to other parties unless it has received specific authorization from the school to do so and it is otherwise permitted by FERPA.
5. **It will not use personally identifiable information in student records to engage in targeted advertising.**
6. **It will provide a means by which a parent, legal guardian, or eligible pupil may review personally identifiable information** in the student's records and correct erroneous information.
7. **It will take actions to help ensure the security and confidentiality of education records,** including but not limited to designating and training responsible individuals on ensuring the security and confidentiality of education records.
8. **It will conduct annual training related to data privacy and security,** including FERPA requirements, for all employees responsible for any aspect of student data management.

9. **It has a data breach procedure in place.** If it knows of a systems security breach that results in an unauthorized disclosure of student personal information, it will comply with relevant state and other data breach laws and will notify the school or agency.
10. **It is willing to include contract provisions or other terms of use detailing rights related to transfer of students' personally identifiable information from education records to the school** or its designated third party upon request by the school or upon expiration or termination of the agreement, and subsequent deletion of students' personally identifiable information held by Securly, Inc. and third parties operating in connection with Securly.
11. **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 school,** separate from any notice in a "click wrap" agreement.

#### **B. California AB 1584 (Buchanan) Privacy of Pupil Records: 3rd-Party Digital Storage & Education Software (Education Code section 49073.1)**

1. **Pupil records obtained by Securly, Inc. from LEA continue to be the property of and under the control of the LEA.**
2. **Securly does not provide a platform by which pupils can create content;** therefore, Securly does not provide a means by which pupils may retain possession and control of such content.
3. **Securly will not use any information in pupil records for any purpose other than those required or specifically permitted by the Securly Service Agreement.**
4. **Parents, legal guardians, or eligible pupils may review personally identifiable information in the pupil's records and correct erroneous information** by contacting the educational institution. District personnel have direct access via the Securly product account login to review pupil data. Securly will provide client with a copy of pupil data, and will modify and/or delete upon written request by the LEA.
5. **Securly is committed to maintaining the security and confidentiality of pupil records.** To that end, Securly 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.
6. **In the event of an unauthorized disclosure of a pupil's records, Securly will promptly notify the educational institution** unless specifically directed not to make such notification by law enforcement. The notification will include: date of the breach, the types of information that were subject to the breach;

general description of what occurred; steps the Securly is taking to address the breach; the contact person at the vendor who the data holder can contact. Securly will keep the client District fully informed until the incident is resolved.

7. **Securly will delete personally identifiable data upon request of the LEA and/or upon expiration of the services agreement.** All data is deleted within 60-days of expiration of services agreement.
  
8. **Securly agrees to work with LEA 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.
  
9. **Securly prohibits using personally identifiable information in pupil records to engage in targeted advertising.**

### C. SB 1177 - Student Online Personal Information Protection Act ("SOPIPA")

1. [Securly does not target advertising on their website or any other website using information acquired from students.](#)
2. [Securly does not use information, including persistent unique identifiers, created or gathered by Securly's site, service, or application, to amass a profile about a K-12 students except in furtherance of K-12 school purposes.](#)
3. [Securly does not and will not sell, rent, or otherwise provide personal information to any third party.](#)
4. [Securly does not disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.](#)
5. [Securly is committed to maintaining the security and confidentiality of pupil records as noted herein.](#)
6. [Securly will delete district-controlled student information when requested by school district.](#)
7. [Securly will disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.](#)

### D. California Education Code § 49073: Collection of Student Information from Social Media

In contracting with education institutions to monitor social posts, Securly, Inc. agrees:

1. [It will gather and maintain only information that pertains directly to school safety or to student safety.](#)
2. [It will not use the information gathered and maintained for purposes other than to satisfy the terms of the contract.](#)
3. [It will not sale or share the information with any person or entity other than the school district, county office of education, charter school, or the student or his or her parent or guardian.](#)
4. [It will destroy the information immediately upon satisfying the terms of the contract.](#)
5. [It will, upon notice and a reasonable opportunity to act, destroy information pertaining to a student when the student turns 18 years of age or is no longer enrolled in the school district, county office of education, or charter school.](#) Securly obtains a list from the school once a year indicating those student who are no longer enrolled and deletes their information accordingly.

## Data Review Process

---

Securly understands that it must respond in a timely manner to school requests to inspect, review, amend or correct personally identifiable information held in education records in cases where such access and change requires Securly's direct involvement and is not otherwise provided for by product functionality available directly to the school. The following is the process for handling such requests:

District personnel have direct access to pupil data via the Securly product account login to review student data.

Parents, legal guardians, or eligible pupils who wish to review personally identifiable information in the student's records and correct erroneous information must contact the educational institution. Securly will provide client with a copy of pupil data, and will modify and/or delete upon written request by the LEA.

Securly has posted within their privacy policy appropriate contact information for comments and questions:

Securly, Inc.

San Jose, CA

support@securly.com



# Security Protocols

---

Securly, Inc. maintains a comprehensive set of security practices that are reasonably designed in accordance with commercial best practices to protect the security, privacy, confidentiality, and integrity of student personal information against risks – such as unauthorized access or use, or unintended or inappropriate disclosure – through the use of administrative, technological, and physical safeguards.

The following is a general overview of Securly, Inc.'s data security protocols:

## Data in Transit

Data is transmitted via HTTPS.

## Data at Rest

Data is encrypted using 256 bit Advanced Encryption Standard (AES).

## Data Storage

Data is stored in Securly's secure Amazon Web Services (AWS) environment. Database backups are also stored on AWS.

## Data Center Security

Securly utilizes data centers operated by Amazon Web Services (AWS) who have extensive experience in designing, constructing, and operating large-scale data centers. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. AWS only provides data center access and information to employees and contractors who have a legitimate business need.

## Personnel

### Training

Securly conducts annual training/review of FERPA, SOPIPA as well as their company privacy and security policies.

### Access

Access to student data is limited to the cloud-operations engineering personnel. All employees with access to student data have undergone background checks.

## Access to Audit

---

Once per year, Securly, Inc. will provide schools with:

audit rights to the school's data

access to the results of Securly's or its third-party security audit

## Product Data List

---

Data Collected for Operation:

General Purpose of Data Collection

	Data Collected for Operation:	General Purpose of Data Collection
1	Student First and Last Name	Required to support product functionality
2	Student ID	Required to support product functionality
3	Parent(s) First and Last Name	Required to support product functionality
4	Parent Email Address	Required to support product functionality
5	School Name	Required to support product functionality
6	School Address	Required to support product functionality
7	Geolocation Data	Non-identifiable mapping displaying generalized location of out-of-school usage for admins.

Note: Securly offers a service that monitors student-generated content across social media platforms and as such gathers and retains student personal data that has been flagged for potential cyberbullying and self-harm based on proprietary algorithms. Emails are not monitored.

Additionally, as part of the web filtering service, Securly captures usage data such as searches made, sites visited, time spent on sites, and access time.

## Third Parties

---

Securly Inc. does not sell, trade, lease or loan the personal information they collect or maintain, in the course of providing Securly's Cloud-based Web Filtering for Schools, to any third party for any reason, including direct marketers, advertisers, or data brokers.

Securly, Inc. 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. Upon request, schools will be provided the names of third parties, if any, with whom student personally identifiable information is shared.

## Accuracy Statement

---

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

Signed and agreed:

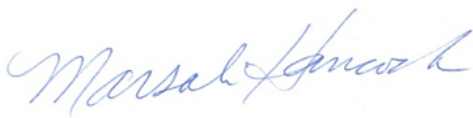


(Signature)

Vinay Mahadik, CEO  
Securly, Inc.

06/20/16

Securly, Inc.'s Cloud based Web Filtering for Schools has been reviewed and found in alignment with the iKeepSafe California Privacy Program Guidelines as indicated by this product profile. Securly, Inc.'s Cloud based Web Filtering for Schools has been awarded the iKeepSafe California Privacy Program badge.



---

(Signature)

Marsali Hancock, President & CEO  
iKeepSafe

06/20/16

## Copyright

---

© 2016 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.

## Disclaimer

---

<sup>1</sup> 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.

You further acknowledge that the California Privacy Assessment Program is not officially recognized by the U.S. Department of Education or any other legislative or regulatory body, and the program does not provide any legal safe harbor. You are encouraged to consult with your attorney. Under no circumstances shall the Internet Keep Safe Coalition, or their Associates be liable for any direct, indirect, incidental, special or consequential damages that result from you not being in compliance with FERPA, SOPIPA, California AB 1584, or for any claim that you are not in compliance with these and other applicable laws. You acknowledge and represent that it is your sole responsibility to evaluate whether or not you are in compliance with these and other laws.