



Aequitas Q Student Information System

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 or not Aequitas Solutions complies with FERPA, SOPIPA, California AB 1584, and other California state laws and district policies as well as the Colorado Student Data Transparency and Security Act. It indicates that Aequitas Solutions has been assessed for and found in alignment with the iKeepSafe Federal, California Privacy Program Guidelines and the Colorado Student Data Transparency and Security Act. Aequitas Solutions has therefore been awarded the iKeepSafe Privacy 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.¹

Product Overview

Aequitas Solutions 'Q': <https://www.myaequitas.com/>

Who We Are - At our core, Aequitas Solutions, Inc. is a K-12 student information system software development, service and support organization.

What We Do – We strive to be a leader in innovative K-12 student information systems. Our mission is two-fold:

- Develop a student information system that:
 - Supports educators in their primary goal, educating students
 - Helps districts streamline operations, process and procedures
 - Supports the way districts work and do business, today and tomorrow
 - Facilitates effective ways to involve parents and other stakeholders in a child's education
- Provide our clients with solutions and services that are unmatched in the K-12 industry

Our Vision – We know the level of effort it takes to manage a student's education from the district office to the home. Our offering must provide all the advantages of today's technology and grow as the industry grows but never lose sight of what we do at our core. We are here to build the best student information system possible. Period. A system that simply works, is functional, easy to use and that helps educators by focusing on what we can do to accomplish our overriding goal; help them to spend more time with their students, not on the system.

Compliance

The 'Q' product is an on--premises SIS solution sold to educational agencies (clients) and, as such, Aequitas

does not collect, store, share or use student data. Aequitas may on occasion have access or exposure to student data for the purposes of client support.

As a participant in the iKeepSafe Privacy Program, Aequitas Solutions, Inc. agrees as applicable to the both the company and the 'Q' product:

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 or educational agency 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 Aequitas is willing to stipulate as such in a contract or terms of use with the school district or educational agency.
3. **It does not operate a platform by which students can 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 or educational agency,** 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 education records to engage in targeted advertising.**
6. **It will provide a means by which a parent, legal guardian, or eligible student 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 Aequitas Solutions, Inc. and third parties operating in connection with Aequitas.

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 or educational agency, 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. Aequitas acknowledges that their agreements with LEAs may allow Aequitas access to private data including pupil records. Pupil records accessed by Aequitas continue to be the property of and under the control of the LEA.
2. Aequitas does not provide a platform by which pupils can create content; therefore, Aequitas does not provide a means by which pupils may retain possession and control of such content.
3. Aequitas will not use any private data, including information in pupil records, for any purpose other than those required or specifically permitted by the services 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 school or educational agency.
5. Aequitas is committed to maintaining the security and confidentiality of pupil records. To that end, Aequitas implements and adheres to the following policies: (i) limiting employee access to student data based on roles and responsibilities; (ii) conducting background checks on employees who have access to student data; (iii) conducting privacy training that includes FERPA for employees with access to pupil data; (iv) protecting personal information with commercially reasonable technical, contractual, administrative, and physical security measures in order to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted private data received from, or on behalf of, Client or its students, to protect it from unauthorized access, release or use.
6. In the event of an unauthorized disclosure of a pupil's records, Aequitas will promptly notify the school or educational agency. The notification will include : (i) the date and nature of the unauthorized use or disclosure; (ii) the data used or disclosed; (iii) general description of what occurred including who made the unauthorized use or received the unauthorized disclosure; (iv) what Aequitas has done or shall do to mitigate any effect of the unauthorized use or disclosure; and (v) what corrective action Aequitas has taken or shall take to prevent future similar unauthorized use or disclosure; (vi) who at Aequitas the client can contact. Aequitas shall provide such other information, including a written report, requested by the client. Aequitas will keep the client fully informed until the incident is resolved.
7. Aequitas will delete personally identifiable data upon request of the LEA and/or upon expiration of the services agreement. At any time upon request or automatically upon termination, cancellation,

expiration or other conclusion of the services agreement, Aequitas shall return all personally identifiable data to client, or if return is not feasible as determined by client in a written notice to Aequitas, destroy any and all personally identifiable data.

8. **Aequitas 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. **Aequitas prohibits using personally identifiable information in pupil records to engage in targeted advertising.**

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

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

D. Colorado Student Data Transparency and Security Act

1. **Aequitas recognizes Student Personally Identifiable Information (SPII)** as defined in the Act as information that, alone or in combination, personally identifies an individual student or the student's parent or family, and that is collected, maintained, generated, or inferred by a public education entity, either directly or through a school service, or by a school service contract provider or school service on-demand provider.
2. **Aequitas agrees to provide clear information that is understandable by a layperson explaining:** (i) the data elements of SPII that it collects; (ii) the learning purpose for which the Aequitas collects the SPII; (iii) and how Aequitas uses and shares the SPII.
3. **Aequitas will provide the information listed in statement 2 above to each public education entity Aequitas contracts with** in a format that is easily accessible through a website. The information will be delivered in the form of this product profile.
4. **Aequitas may make available the information listed in statement 2 on the Aequitas website in the form of this product profile.**
5. **Aequitas recognizes and adheres to obligations outlined in the ACT with respect to data usage and security as addressed in herein.**

Data Review Process

Aequitas Solutions, Inc. 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 Aequitas Solutions' direct involvement and is not otherwise provided for by product functionality available directly to the school.

The Aequitas Solution system provides for direct access:

At the client's discretion, the 'Q' product may be configured to allow any authorized user to permit parents, legal guardians, and eligible pupils to review personally identifiable information contained in private data, and to correct erroneous information, in accordance with procedures established by the client.

Security Protocols

Aequitas Solutions, 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 Aequitas Solutions’ data security protocols:

Data in Transit

Transfer of data is controlled by the client. Aequitas Solutions’ recommendation to the client is that all interactions should occur via HTTPS.

Data at Rest

Data is stored in a SQL Server database housed by the client. Access to the database is completely controlled by the client.

Access through the application includes authentication using internally encrypted passwords or Active Directory/LDAP over secure channels. All user access is controlled via internal permissions and roles.

Personnel

Training

Aequitas conducts annual privacy and security training for all employees.

Access

Access to student data is role--based; limited to those employees who need access to perform job responsibilities such as customer support. All employees with access to student data have undergone background checks.

Access to Audit

Once per year, Aequitas Solutions, Inc. will provide schools upon request with:

- audit rights to the school’s data
- access to the results of Aequitas Solutions, Inc.’s or its third--party security audit

Product Data List

The 'Q' product is a full-featured SIS that includes core functionality such as enrollment, attendance, scheduling and grades. It is an on-premises solution and, as such, Aequitas does not collect, store, share or use any student data. Data is collected by the client that has entered into a services agreement to use the 'Q' product. Data is stored in a SQL Server database housed by those clients.

Aequitas may have limited contact with student data for the purpose of troubleshooting the Q application. Additionally, Aequitas's policy is to perform a munge function against any client database to de-identify and protect student data.

Third Parties

Aequitas 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.

Aequitas does not contract with other third-party companies to perform business functions or services on their behalf and, therefore, does not share any PII with such third parties.

Accuracy Statement

Aequitas Solutions, 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)

Randy Robertson
Aequitas Solutions, Inc.

06/03/2022

Aequitas Solutions, Inc. has been reviewed and found in alignment with the iKeepSafe California Privacy Program Guidelines as indicated by this product profile. Aequitas Solutions, Inc. has been awarded the iKeepSafe California Privacy Program badge.

DocuSigned by:



4936610B3823488...

(Signature)

Amber Lindsay
President and CEO
Internet Keep Safe Coalition (iKeepSafe)

06/03/2022

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

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.

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.