iKeepSafe Product Profile QoreInsights

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 QoreInsights complies with FERPA and IL SOPPA. It indicates that QoreInsights has been assessed for alignment with the iKeepSafe Program Guidelines.

Product Overview

Product: QoreInsights

https://QoreInsights.com/

The Classroom Education Plan (CEP) is central to QoreInsight's mission to make evidence-based instruction and equitable outcomes a reality, at scale. The CEP is a decision support and workflow-embedded professional development system to aid teachers' implementation and monitoring of evidence-based instructional strategies in elementary math and literacy. The CEP uses whole-child data to identify a classroom's most urgent needs in both academic and underlying non-academic factors associated with learning (e.g., socio-emotional, executive function, and foundational learning skills), incorporates decision intelligence algorithms to recommend integrated evidence-based literacy strategies to address those needs, and provides multiple guided learning opportunities to deepen teachers' expertise and implementation.

Agreement

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

1. Student records obtained by QoreInsights 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 QoreInsights.
2. QoreInsights users may retain possession and control of their own generated content.
3. QoreInsights will not use any information in a student record for any purpose other than those required or specifically permitted by the QoreInsights 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, QoreInsights users may access, correct, update, or delete personal information in their profile by signing into QoreInsights, accessing their QoreInsights account, and making the appropriate changes.
5. QoreInsights 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, QoreInsights will promptly notify users unless specifically directed not to provide such notification by law enforcement officials.
7. QoreInsights 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. QoreInsights 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. QoreInsights prohibits using personally identifiable information in student records to engage in targeted advertising.
10. QoreInsights 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.

B. As related to the Student Online Personal Protection Act, 105 ILCS 85/- (SOPPA) , QoreInsights agrees:

Sec. 10. QoreInsights shall not knowingly do any of the following:

(1) Engage in targeted advertising on the operator's site, service, or application or target advertising on any other site, service, or application if the targeting of the advertising is based on any information, including covered information and persistent unique identifiers, that the operator has acquired because of the use of that operator's site, service, or application for K through 12 school purposes.

(2) Use information, including persistent unique identifiers, created or gathered by the operator's site, service, or application to amass a profile about a student, except in furtherance of K through 12 school purposes. "Amass a profile" does not include the collection and retention of account information that remains under the control of the student, the student's parent, or the school.

(3) Sell or rent a student's information, including covered information. This subdivision (3) does not apply to the purchase, merger, or other type of acquisition of an operator by another entity if the operator or successor entity complies with this Act regarding previously acquired student information.

(4) Except as otherwise provided in **Section 20 of this Act,** disclose covered information, unless the disclosure is made for the following purposes:

(A) In furtherance of the K through 12 school purposes of the site, service, or application if the recipient of the covered information disclosed under this clause (A) does not further disclose the information, unless done to allow or improve operability and functionality of the operator's site, service, or application.

(B) To ensure legal and regulatory compliance or take precautions against liability.

(C) To respond to the judicial process.

(D) To protect the safety or integrity of users of the site or others or the security of the site, service, or application.

(E) For a school, educational, or employment purpose requested by the student or the student's parent, provided that the information is not used or further disclosed for any other purpose.

(F) To a third party if the operator contractually prohibits the third party from using any covered information for any purpose other than providing the contracted service to or on behalf of the operator, prohibits the third party from disclosing any covered information provided by the

operator with subsequent third parties, and requires the third party to implement and maintain security procedures and practices as required under Section 15.

Sec. 15. QoreInsights shall do the following:

(1) Implement and maintain reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect covered information from unauthorized access, destruction, use, modification, or disclosure.

(2) Delete, within a reasonable time period, a student's covered information if the school or school district requests deletion of covered information under the control of the school or school district, unless a student or his or her parent consents to the maintenance of the covered information.

(3) Publicly disclose material information about its collection, use, and disclosure of covered information, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.

(4) Except for a nonpublic school, for any operator who seeks to receive from a school, school district, or the State Board in any manner any covered information, enter into a written agreement with the school, school district, or State Board before the covered information may be transferred. **The written agreement may be created in electronic form and signed with an electronic or digital signature or may be a click wrap agreement that is used with software licenses, downloaded or online applications and transactions for educational technologies, or other technologies in which a user must agree to terms and conditions before using the product or service.** Any written agreement entered into, amended, or renewed **must contain all of the following:**

(A) A listing of the **categories or types of covered information t**o be provided to the operator.

(B) A statement of the **product or service being provided** to the school by the operator.

(C) A statement that, pursuant to the federal Family Educational Rights and Privacy Act of 1974, **the operator is acting as a school official with a legitimate educational interest**, is performing an institutional service or function for which the school would otherwise use employees, under the direct control of the school, with respect to the use and maintenance of covered information, and is using the covered information only for an authorized purpose and may not re-disclose it to third parties or affiliates, unless otherwise permitted under this Act, without permission from the school or pursuant to court order.

(D) A description of how, if a **breach is attributed to the operator, any costs and expenses incurred by the school in investigating and remediating the breach will be allocated between the operator and the school.** The costs and expenses may include, but are not limited to:

(i) providing notification to the parents of those students whose covered information was compromised and to regulatory agencies or other entities as required by law or contract;
(ii) **providing credit monitoring to those students whose covered information was exposed in a manner during the breach that a reasonable person would believe that it could impact his or her credit or financial security;**
(iii) legal fees, audit costs, fines, and any other fees or damages imposed against the school as a result of the security breach; and
(iv) **providing any other notifications or fulfilling any other requirements adopted by the State Board or of any other State or federal laws.**

(E) A statement that the operator must delete or transfer to the school all covered information if the information is no longer needed for the purposes of the written agreement **and to specify the time period** in which the information must be deleted or transferred once the operator is made aware that the information is no longer needed for the purposes of the written agreement.

(F) **If the school maintains a website**, **a statement that the school must publish the written agreement on the school's website**. If the school does not maintain a website, **a statement that the school must make the written agreement available for inspection by the general public at its administrative office**. If mutually agreed upon by the school and the operator, provisions of the written agreement, other than those under subparagraphs (A), (B), and (C), may be redacted in the copy of the written agreement published on the school's website or made available at its administrative office.

(5) In case of any breach, within the most **expedient time** possible and without unreasonable delay, but no later than **30 calendar days after the determination that a breach has occurred**, notify the **school of any breach of the students' covered information.**

(6) Except for a nonpublic school, **provide to the school a list of any third parties or affiliate**s to whom the operator is currently disclosing covered information or has disclosed covered information. This list must, at a minimum, be updated and provided to the school by the **beginning of each State fiscal year and at the beginning of each calendar year.**

Data Review Process

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

The Educational Institution determines the information collected, maintained, and processed using QoreInsights' services. The Educational Institution retains the right to review, modify, and/or refuse to permit further collection or use of student data information at any time. The Educational Institution uses QoreInsights' services to assist with the administration of school-related activities and to provide a streamlined way to collect, organize, access, and report information for educational purposes. These uses are specific to each Educational Institution and are governed by the contract between QoreInsights and the Educational Institution. If there are any questions regarding the collection, storage, and use of the information the Educational Institution shares with QoreInsights, please contact the Educational Institution directly.

General inquiries related to privacy may be directed to:

QoreInsights

By Email: *Questions@QoreInsights.com*
By Mail: QoreInsights Inc, 9935-D Rae Road, #252, Charlotte, NC 28277
By Phone: 704-540-5252

Security Protocols

QoreInsights 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

All data is transmitted securely via HTTPS, specifically the more secure TLS 1.3 protocol.

Data at Rest

QoreInsights' data storage is provided by Microsoft Azure Encryption methodology is inherent in their data storage systems. And, is replicated in encrypted form for backup and disaster recovery.

Data Center Security

QoreInsights uses Microsoft Azure Data Centers and these centers conform to the following:

By following the standards of ISO/IEC 27001 and the code of practice embodied in ISO/IEC 27018, Microsoft demonstrates that its privacy policies and procedures are robust and in line with its high standards.

Customers of Microsoft cloud services know where their data is stored. Because ISO/IEC 27018 requires certified CSPs to inform customers of the countries in which their data may be stored, Microsoft cloud service customers have the visibility they need to comply with any applicable information security rules.

Customer data won't be used for marketing or advertising without explicit consent. Some CSPs use customer data for their own commercial ends, including for targeted advertising. Because Microsoft has adopted ISO/IEC 27018 for its in-scope enterprise cloud services, customers can rest assured that their data will never be used for such purposes without explicit consent, and that consent cannot be a condition for use of the cloud service.

Microsoft customers know what's happening with their PII. ISO/IEC 27018 requires a policy that allows for the return, transfer, and secure disposal of personal information within a reasonable period of time. If Microsoft works with other companies that need access to your customer data, Microsoft proactively discloses the identities of those sub-processors.

Microsoft complies only with legally binding requests for disclosure of customer data. If Microsoft must comply with such a request (as in the case of a criminal investigation), it will always notify the customer unless it is prohibited by law from doing so.

Please see more information below in the available link:

https://azure.microsoft.com/en-us/overview/trusted-cloud/privacy/

Personnel

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

Training: Employees of QoreInsights 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, QoreInsights will provide schools with:

[X] audit rights to the school's data

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

Data Breach

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

QoreInsights 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 Deletion

QoreInsights states they will retain personal identifiable information for as long as the account is active, or as needed to provide their users with their services. Please contact them at the email address at Support@QoreInsights.com should someone wish to cancel their account or request that we no longer use the information to provide services. They will retain and use the information as necessary to comply with their legal obligations, resolve disputes, and enforce their agreements.

Research

QoreInsights stated they use none of the customer data for research or statistical purposes at this time. If they use any customer database for troubleshooting or conducting research, the data is de-identified and no Student PII is available to view.

Additionally, as part of this use of information, they may provide aggregate information to partners about how our users, collectively, use our site. They may share this type of statistical data so that their partners also understand how often people use their partners' services and the Website to help provide the user with an optimal online experience.

Third Parties

QoreInsights 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.

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

QoreInsights utilizes the following third-party vendors:

Third Party	Purpose	Information Shared
Azure	Cloud-based hosting	All information in the system

Classlink	Single sign-on intermediary to integrate CEP with schools	All information in the system

Product Data List

Data Collected	General Purpose of Data Collec
STUDENT FIRST AND LAST NAME	Required to support product funct
OTHER STUDENT ID	Required to support product funct
SCHOOL NAME	Required to support product funct
SCHOOL ADDRESS	Required to support product funct
OTHER PERSISTENT IDENTIFIER	Required to support product funct
ACCESS TIME	Analytics
TIME SPENT ON SITE	Analytics
PAGE VIEWS	Analytics

Accuracy Statement

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

Signed and agreed:

(Signature)

Toni Shub, EdD
Founder and CEO
www.qoreinsights.com
www.pathwaysforlearning.com

09/15/2022

The QoreInsights service has been reviewed and found in alignment with iKeepSafe's FERPA and IL SOPPA Privacy Program Guidelines as indicated by this product profile. QoreInsights has been awarded the iKeepSafe FERPA Privacy Program badges.

DocuSigned by:
Amber Lindsay
4936610B3823488...

(Signature)

Amber Lindsay
President & CEO
iKeepSafe

09/15/2022