iKeepSafe

iKeepSafe Product Profile
Giving-Tree Associates, LLC
T/A Passport For Good ("PFG")

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, share, process or otherwise handle student data.

This *iKeepSafe Product Profile* is intended to assist you in determining whether PFG complies with COPPA and FERPA. It indicates that PFG has been assessed for alignment with the iKeepSafe FERPA and COPPA Guidelines.

Product Overview

PFG is an easy to use website and mobile app designed to capture a student's community service, internships, clubs, event participation and other student activities both in the classroom and outside of school. In the education market, a key target market for PFG is K-12 students ("Students"). PFG is also working with colleges, Greek societies, corporations, associations and nonprofits. PFG provides students with a personal profile (the "Passport") of their community service and
activities that they can carry with them. PFG also provides a seamless method for Students to obtain verification of community service hours for graduation or other school requirements.

Students can access PFG two ways 1.) as a registered user associated with a school subscribing to PFG; or 2.) as an individual downloading the app thru an app store (IOS and Android).To register as a user an individual would provide 3 points of information; name, email and date of birth. Students under the age of 18 years, not associated with a subscribing school may use PFG independent of a subscribing school with verifiable parental consent. Students registering as a user who are members of a subscribing school can use PFG for educational purposes and under the school official exception the student users do not need to provide separate verifiable parental consent.

Once registered the student can input data on community service, career development and activities both through the school and external to the school. The input collected includes hours, a rating of the event, a journal entry, name and location of the event, the supervisor of the event (name, address, phone and email) and date of event.

PFG is not a social media tool.

Students and schools can download data. Student data is not deleted unless requested by the student or parent of the student user. Schools have access to student data provided the school continues to subscribe to PFG as an institution user and the student continue to be associated with the school and registered with PFG. Once a school no longer subscribes to PFG and is no longer a user the school cannot access any new student data.

Students can leave one subscribing school institution and continue with a new subscribing institution (e.g., high school to college) provided the students join the new subscribing institution and are registered users.

PFG's offerings are built using the following software stack: net mvc / web api , azure sql db , redis, elk, ionic mobile app.

Agreement

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

Student records obtained by PFG 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 student records it provides to PFG.

1. PFG users retain possession and control of their own generated content. The user's content on PFG belongs to the user and exists outside of any institution.
2. PFG will not use any information in a student record for any purpose other than those required or specifically permitted by the PFG Terms and Privacy Policy appearing on the PFG site.
3. Parents, legal guardians, or eligible students may review personally identifiable information ("PII") in the student's records and correct erroneous information by contacting their educational institution. Additionally, PFG users may access, correct, update, or delete information in their profile by signing into PFG, accessing their PFG account, and making the appropriate changes.
4. PFG is committed to maintaining the security and confidentiality of student records. Towards this end, PFG take the following actions:
    a. PFG limits employee access to student data to only those employees with a need to have such access to fulfill their job responsibilities;
    b. PFG conducts background checks on our employees that have access to student data;
    c. PFG conduct regular employee privacy and data security training and education; and
    d. PFG protect PII with technical, contractual, administrative, and physical security safeguards of a user's account in order to protect against unauthorized access, release or use.
5. In the event of an unauthorized disclosure of a student's records, PFG will notify affected parties, as soon as reasonably possible after confirmation of the unauthorized disclosure and the ability to ascertain the information required to notify the affected parties, unless specifically directed not to provide such notification by law enforcement officials.

6. PFG will delete data including PII as soon as reasonably possible upon receipt of a request from a user or parent of a user in writing requesting deletion. When data is deleted it may be erased or sufficiently anonymized in accordance with PFG's policies.
7. PFG agrees to work with educational institutions to ensure compliance with FERPA including 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.
8. PFG prohibits using PII in student records to engage in targeted advertising.
9. PFG will not make material changes to PFG Terms or Privacy Policy, including making significant changes impacting the collection, use, sharing, disclosure or retention of data collected without prior notice to its users.

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

1. PFG contracts directly with schools and, as such, may rely on consent from the school instead of the parents for collection of PII from children when data collected is for the use and benefit of the school, and not for any other commercial purposes.

2. PFG makes available clearly written policies explaining what data it collects from users, how such data is used, shared, stored and to whom it may be disclosed.

3. PFG makes available a copy of the Privacy Policy including the K-12 Privacy Policy, if applicable to the school prior to completion of the licensing, download or installation of the software.

4. PFG provides the school with a description of the types of PII collected; an opportunity, upon request by the child or parent to review the child's PII and/or have the PII deleted; and the opportunity to prevent further use, sharing or online collection of a children's PII.

5. PFG 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. PFG does not/will not condition a child's participation in an activity on the child disclosing more PII than is reasonably necessary to participate in such activity.

7. PFG maintains reasonable procedures to protect the confidentiality, security, and integrity of PII collected from children. It takes reasonable steps to release children's PII only to third party service providers 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. PFG only stores a user's data, including PII for as long as the account is active, and it is necessary to provide services to the user. PFG deems an account and data including PII, inactive if a user does not log into their account for a period of 7 years. PFG will delete data including PII as soon as reasonably possible upon receipt of a request from a user or parent of a user in writing requesting deletion. When data is deleted it may be erased or sufficiently anonymized in accordance with PFG policies.

9. PFG 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 PFG offerings. Such training will include all

employees who are directly or peripherally involved in collection, use, storage, disclosure or any other handling of data.

10. PFG 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. PFG will notify schools of material changes to its Privacy Policy that affect the collection or use of PII from children.

Data Review Process

Parents are encouraged to work directly with teachers and school to make any changes in their data. If however, a parent needs to get in touch with PFG, they can write to support@passportforgood.com and PFG will work with the school and do it's best to make the required changes.

Teachers, administrators and parents can directly edit certain information in their PFG profiles. Schools also have a right to use any other similar service and can place a request to get all of their data. PFG will do our best to comply with such requests.

General inquiries related to privacy may be directed to:
Gayle Farman, Founder & CEO
333 Broadway Troy,
New York 12180
*Phone: (*518) 852-7208
E-Mail: gayle@passportforgood.com

Security Protocols

PFG 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:

HTTPS encrypted

Data at Rest:

PFG uses a Microsoft Azure SQL DB to store its data. Transparent Data Encryption (TDE) encrypts SQL Server, Azure SQL Database, and Azure SQL Data Warehouse data files, known as encrypting data at rest. At a high level it uses an AES encryption and a key.

Data Center Security:

PFG uses Microsoft Azure Data Centers for all Data Storage.

Please see the article from Microsoft for details on the Azure datacenters, including physical infrastructure and security.

https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

Personnel:

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

Training: Employees of PFG with access to student data will receive annual privacy and security training that includes FERPA and COPPA.

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

PFG stores all data, including PII with Microsoft Azure and relies upon the security audits conducted by Microsoft Azure. PFG reviews the security audits conducted by Microsoft Azure on a regular basis or as needed. Annually, PFG will allow schools access to the results of the Microsoft Azure security audits.

Data Breach

In the event of an unauthorized disclosure of a student's records, PFG will notify affected users, as soon as reasonably possible after confirmation of the unauthorized disclosure and the ability to ascertain the information required to fulfill the notice requirements, unless specifically directed not to provide such notification by law enforcement officials.

Notification shall identify:

a. The date the breach was discovered;
b. The date of the breach, estimated date of the breach or the date range within the breach occurred or a best estimate;
c. The information that was subject to the breach;
d. A general description of what occurred including how the breach occurred and the number of affected individuals, based on the available information;
e. The name of the contact person at PFG;
f. Whether the notification was delayed because of law enforcement;
g. What steps PFG has taken to respond to and mitigate the situation, prevent it from happening again, and advice to the impacted individuals on how they can best protect themselves; and
h. Contact information for representatives who can assist individuals, parents or eligible students with additional questions.

Data Deletion

PFG may store, collect, use students' data, including, PII, for as long as the account is active and it is necessary to provide services to the user unless a user or a user's parent or guardian has specifically requested deletion of data, including, PII, in whole or in part, by PFG. PFG will delete data including PII as soon as reasonably possible upon receipt of a request from a user or parent of a user in writing requesting deletion. PFG deems an account and data including PII, inactive if a user does not log into their account for a period of 7 years. When data is deleted it may be erased or sufficiently anonymized in accordance with PFG policies.

You must contact PFG personally and in writing in reference to deleting any of your data, including, PII in whole or in part, from the Site and the PFG App as follows:

Gayle Farman, Founder & CEO
333 Broadway Troy,
New York 12180
Phone: (518) 852-7208
E-Mail: gayle@passportforgood.com

Research

PFG may engage in research and in such cases will mask, de-identify, anonymize and/or aggregate the data, including PII. PFG only uses end user data to debug customer specific issues. PFG does not use user data for production improvement or research. PFG does not use user data in any non-production environments including testing, development and training.

Third Party Service Providers

PFG does not sell, trade, lease or loan the PII PFG collects or maintains, in the course of providing the service, to any third-party service provider for any reason, including direct marketers, advertisers, or data brokers.

PFG contracts with other third-party service providers to perform business functions or services on PFG's behalf and may share PII with such third parties as required to perform those functions. PFG has agreements in place with all third-party service providers with access to PII to ensure they only use the PII for purposes necessary to deliver the authorized service and to ensure they maintain the confidentiality and security of the PII. The agreements align with PFG' data privacy and security policies and expectations.

Product Data List -Personally Identifiable Information

Data element	**Purpose of Data Collected**
Student First and Last Name	Product Functionality
Student Email Address	Product Functionality
Student phone number/mobile	Product Functionality
Student Password	Product Functionality
Student Age/DOB	Product Functionality
Grade Year	Product Functionality
Other Student ID	Product Functionality
School Name	Product Functionality
Team/Clubs	Product Functionality
Video, Photographs	Product Functionality
Browser Type	Analytics
Access Time	Analytics
Time spent on Site	Analytics
Page Views	Analytics
Referring URL's	Analytics

New York State Education Law §2-d

1. PFG does not sell or release any student PII for any commercial or marketing purposes.
2. PFG agrees to work with educational institutions to ensure compliance with FERPA including providing parents with the ability to inspect and review student records maintained by PFG. The right of inspection is consistent with FERPA.
3. A complete list of all student data collected by PFG is available for review by parents by contacting PFG.
4. Parents may review PII in the student's records and correct or delete information by contacting their educational institution.
5. PFG takes reasonable steps to release children's PII only to third party service providers 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. See Third Party Service Providers section above.

6. PFG has a comprehensive Security Program in place designed to protect the confidentiality, integrity and availability of systems, networks and data. See Security Protocols section above.
7. When PFG service to a school is completed, records containing PII may be destroyed in accordance with our data deletion and retention statements above.

PFG hereby confirms the accuracy and truthfulness of all information contained in the PFG *iKeepSafe Product Profile* and has authorized iKeepSafe to make the PFG *iKeepSafe Product Profile* available upon request to any interested schools.

Signed and agreed:

(Signature)
Founder & CEO
Gayle Farman
333 Broadway Troy,
New York 12180
Phone: (518) 852-7208
E-Mail: gayle@passportforgood.com

08/22/2019

The PFG service as well as the site, the PFG app and software running the site and PFG app been reviewed and found in alignment with iKeepSafe's FERPA and COPPA Guidelines as indicated by the PFG iKeepSafe Product Profile. PFG has been awarded the iKeepSafe FERPA and COPPA Privacy Program badges. iKeepSafe has also reviewed the site, the PFG app and software running the site and app and have found in alignment with New York State Ed Law 2d.

DocuSigned by:
Amber Lindsay
4936610B3823488...

(Signature)

Amber Lindsay
iKeepSafe Vice President
phone: 801.472.6175
website: ikeepsafe.org/
09/18/2019

Copyright