Prodigy Math Game

iKeepProfile

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 Prodigy Math Game (hereinafter referred to as "Prodigy") complies with FERPA, COPPA, SOPIPA, California AB 1584, and other California state laws and district policies. It indicates that Prodigy has been assessed for and found in alignment with the iKeepSafe California Privacy Program Guidelines and COPPA Safe Harbor Guidelines. Prodigy has therefore been awarded the iKeepSafe California Program badge and COPPA Safe Harbor Seal.

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

Prodigy: https://prodigygame.com/

Prodigy is a FREE, highly engaging math game that's used by over 10,000,000 students in North America. It's fully aligned to the Common Core, Texas, Florida, and Ontario Math Standards for Grades 1-8 and automatically differentiates for each child. Educators can easily create formative assessments, track trouble spots, and view teacher/admin reports in real-time.

Compliance

As a participant in the iKeepSafe California Privacy Program, Prodigy 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 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 Prodigy is willing to stipulate as such in a contractor 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 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 Prodigy and third parties operating in connection with Prodigy.
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 AB1584 (Buchanan) Privacy of Pupil Records: 3rd-Party Digital Storage & Education Software (Education Code section 49073.1)

1. Pupil records obtained by Prodigy from LEA continue to be the property of and under the control of the LEA.
2. Prodigy does not provide a platform by which pupils can create content; therefore, Prodigy does not provide a means by which pupils may retain possession and control of such content.
3. Prodigy will not use any information in pupil records for any purpose other than those required or specifically permitted by the contract for Prodigy's services.
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. Prodigy's system enables any authorized user to permit parents, legal guardians, and eligible pupils to review personally identifiable information contained in pupil records, and to correct erroneous information, in accordance with procedures established by the school or educational agency.
5. Prodigy is committed to maintaining the security and confidentiality of pupil records. To that end, Prodigy 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, COPPA, SOPIPA, & California AB 1584 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, Prodigy will promptly notify the school or educational agency. The notification will include: date of the breach, the types of information that were subject to the breach; general description of what occurred; steps Prodigy is taking to address the breach; the contact person at the vend or who the data holder can contact. Prodigy will keep the client fully informed until the incident is resolved.
7. Prodigy will delete personally identifiable data upon request of the LEA and/or upon expiration of the services agreement. Upon the termination of a service contract, Prodigy will isolate and permanently delete pupil records belonging to the school district or educational agency unless the school, educational agency, or applicable regulations require the retention of such data, in which case the records shall be deleted upon the expiration of the retention period. Prior to deleting any pupil records, Prodigy will ensure the school district or educational agency has downloaded backups of the data.
8. Prodigy 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. Prodigy prohibits using personally identifiable information in pupil records to engage in targeted advertising.

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

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

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

1. Prodigy 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. Prodigy 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. Prodigy 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. Prodigy 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. Prodigy collects 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. Prodigy does not/will not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity.
7. Prodigy 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 are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.
8. Prodigy retains personal information collected online from a child for 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. Prodigy 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. Prodigy 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

Prodigy 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 Prodigy's direct involvement and is not otherwise provided for by product functionality available directly to the school.

The Prodigy system provides for direct access:

The Prodigy system enables any authorized user to permit parents, legal guardians, and eligible pupils to review personally identifiable information contained in pupil records, and to correct erroneous information in accordance with procedures established by the school or educational agency.

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 school or educational agency.

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

support@prodigygame.com
1100 Burloak Drive, Suite 200
Burlington, ON L7L 6B2
1 866 585 4655

Security Protocols

Prodigy 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 Prodigy's data security protocols:

Data in Transit

Data is encrypted in transit, no uploads are currently allowed from services, but if supported, are done over HTTPS. Any internal file uploads are done over SFTP, FTP is disabled on all systems

Data at Rest

- Password Protection
- SSL Encryption
- Salted hashing
- Independent service level APIs
- Database protection
- Periodic data review

Data Storage

- AWS's United States Regions
    - US East (N. Virginia)
- Azure: Data is stored in Microsoft's U.S. and Canadian regions:
    - US East (Virginia), Central US (Iowa)

Personnel

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.

Product Data List

Data Collected for Operation	*General Purpose of Data Collection*
Student First and Last Name	Required to support product functionality
Parent(s) First and Last Name	Required to support product functionality
Parent Email Address	Required to support product functionality
Parent Password	Required to support product functionality
Geolocation	Required to support product functionality
Browser Type	Business Intelligence
Access Time	Business Intelligence
Time Spent on Site	Business Intelligence
Page Views	Business Intelligence

Third Parties

Prodigy 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.

Prodigy 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. Prodigy 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.

Prodigy utilizes the following third party vendors as indicated below.

Hosting

- Microsoft Azure: Cloud hosting service data for the game and website
- Amazon Web Services: Cloud hosting service data for the game and website
- Datadog: Hosting analytics service used to track network usage and health
- Github: Code repository service contains all code for the game and website
- Npm: Binary module hosting system used to host code that is used by internal services
- Atlassian Bitbucket: Code repository service contains all code for the game and website
- Pingdom: Website status monitoring service used to alert us if/when our website is down

Payment

- iTunes: Online apps and payment platform used to host Prodigy's iOS app and collect payments from iTunes users.
- Stripe: Online payment platform all credit card information and transaction details for premium memberships upgrades

- Shopify: Online ecommerce platform all toy sales are processed through this site

Email and Video Marketing

- Mailchimp: Email marketing service used to send bulk emails to teachers/parents
- SendWithUs: Email marketing service used to template and schedule our email campaigns
- Sparkpost: Email delivery service for sending emails to users
- Wistia: Video tracking software used to track which tutorial videos are being clicked on most frequently and how users are interacting with these videos

Analytics

- Google Analytics: used to track various non-identifiable information about users.
- Mixpanel: Website analytics service used to track user interactions with website and trigger corresponding emails.
- Streak: CRM software for Gmail used to track school administrators' progress through sales funnel
- Yesware: Email analytics service used to track delivery of personal emails and schedule mailmerges

iKeepSafe technical assessment indicated appropriate use of 3rd parties for product functionality and analytics.

Accuracy Statement

Prodigy 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:

DocuSigned by:
Rohan Mahimker
92282EE9E7BD41E...

1/6/2017

Rohan Mahimker, co-CEO
Prodigy Math Game

Prodigy has been reviewed and found in alignment with the iKeepSafe California Privacy Program Guidelines and COPPA Safe Harbor Guidelines as indicated by this product profile. Prodigy Math Game has been awarded the iKeepSafe California Privacy Program badge and the COPPA Safe Harbor Seal.

Signed and agreed:

DocuSigned by:
Holly Hawkins
4936610B3823488...

12/22/2016

Holly Hawkins, Chief Safety & Privacy Officer
iKeepSafe

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. 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.