IKEEPSAFE COPPA SAFE HARBOR PROGRAM APPLICATION EXHIBIT I

About The Internet Keep Safe Coalition (iKeepSafe):
iKeepSafe was established in 2005 as a 501(c)3 nonprofit alliance of more than 100 policy leaders, including governors, attorneys general, educators, law enforcement members, technology experts and public health professionals.

Through this network of support, iKeepSafe tracks global trends and issues surrounding digitally connected products and their effect on children. This research drives the continuous creation of positive resources for parents, educators and policymakers to teach children how to use new technologies and the Internet in safe and healthy ways.

iKeepSafe works with industry, education, government and policy leaders exploring concerns related to online privacy, security, safety and compliance. iKeepSafe's Board of Directors includes nationally recognized thought leaders in online privacy, security, ethics, law, liability, health, and safety.[1]

iKeepSafe was founded by Jacalyn Leavitt, who served as Utah's 14th First Lady from 1993 to 2003. The trademarks of her public service have always been improving the health, safety and literacy rates of children. The organization operates under the leadership of its President and CEO, Holly Hawkins, who has more than 20 years' child safety experience in both for profit and nonprofit sectors, she has developed national prevention programs, designed best practices for youth protection and privacy, and built national awareness campaigns.

Ms. Hawkins comes to iKeepSafe after serving most recently as Vice President of Programs and Outreach at the National Center for Missing and Exploited Children (NCMEC). In her role at the NCMEC, Ms. Hawkins was the leading force behind the development of KidSmartz, a national abduction prevention program for children in grades K-5. She also oversaw the expansion of NetSmartz, a leading Internet safety program, and the development of trainings for law enforcement, educators and other professionals focused on reducing child sexual exploitation and preventing child victimization.

Prior to NCMEC, Ms. Hawkins served as AOL's Director of Global Consumer Policy and Child Safety where she worked closely with both domestic and international child protection and Internet safety organizations to develop best practices for the protection of children online. She was responsible for a wide range of consumer protection and risk management issues for AOL brands including children's safety and privacy, programming and advertising policies as well as community standards and moderation.

Ms. Hawkins served on the National Coalition to Prevent Child Sexual Abuse and Exploitation, the board of the Family Online Safety Institute and was an advisor to Enough is Enough. She was also a member of the European Commission's Social Networking Principles Task Force, Internet Watch Foundation and the UK Council for Children and Internet Safety (UKCCIS). Ms. Hawkins is a Certified International Privacy Professional (CIPP/US).

[1] http://www.ikeepsafe.org/about-us/board-of-directors/
[2] http://www.ikeepsafe.org/educators/fauxpaw/

iKeepSafe's Compliance Experience:

iKeepSafe has a strong history in the compliance space, providing almost a decade of leadership in areas ranging from E-rate funding requirements around online safety education, to professional development training around ethical, responsible and legal integration of technology in the classroom. The flagship Generation Safe™[3] program provides education and training to school leadership on compliance assessment, incident response, policy and safety. Its goal is to help schools navigate the digital environment, protect them from liability and safely integrate technology into existing school initiatives.

[3] Generation Safe™ Professional Development program brought iKeepSafe experts to school campuses across multiple states and abroad to train stakeholders on managing digital incidents, such as cyberbullying, sexting and plagiarism, while protecting the privacy of individuals and organizations. http://generationsafe.ikeepsafe.org/

iKeepSafe COPPA Safe Harbor - Privacy Compliance Advisors
iKeepSafe utilizes trained employees and consultants certified by the International Association of Privacy Professionals and/or attorneys by trade working in the privacy field.

iKeepSafe Seal Program Mission Within the Education Community:
The iKeepSafe Safe Harbor seal program is intended to provide operators of websites and online services with guidance to ensure effective compliance with COPPA requirements. In addition, consistent with iKeepSafe's long-standing mission of providing resources that serve the needs of the education community, iKeepSafe is also offering special, optional features in the form of additional certification programs, designed to ensure that technology brought into the classroom meets the highest standards of privacy.

These features will take the form of:

- Privacy assessments and education for website and online service operators and data management vendors related to the Family Educational Rights and Privacy Act (FERPA)

- Education and training certification programs for school personnel focused on COPPA and FERPA requirements, and the responsibilities of teachers, administrators and other school district employees bringing technology into schools

These features are not specific to operator requirements around COPPA or the iKeepSafe Safe Harbor program, and so they are not detailed further in this application. However, they are intended to provide guidance and resources to the business and education communities on how to best ensure that the technology brought into the classroom is aligned with privacy requirements.

[4] http://www.ikeepsafe.org/educators/schoolprivacy/
[5] http://www.ikeepsafe.org/educators/datasecurity/
[6] http://www.ikeepsafe.org/educators/byod/

EXHIBIT II
(Per § 312.11(b)(1) and (c)(1))

General Statement of Program Requirements
The iKeepSafe Safe Harbor program assists operators of websites and online services that are – in whole or in part – directed to children under the age of 13. The program is designed to help ensure that practices surrounding collection, use, maintenance and disclosure of personal information from children are consistent with principles and requirements of the Children's Online Privacy Protection Act (COPPA) and general tenants of iKeepSafe's mission to encourage healthy and safe use of the Internet.

A. Guiding Principles
The iKeepSafe Safe Harbor program has been developed around the following 5 guiding principles to help companies ensure compliance with the requirements of the Children's Online Privacy Protection Act:

1. Transparency
   Clearly written policies explaining what data a website or online service collects from users, how such data is used and stored, and to whom it may be disclosed are mandatory. Such policies must accurately reflect actual website or online service data handling practices, and must be easy for the user to find and understand.

2. Minimization of Data Collection
   In the arenas of product development, media and marketing intended for children, collection of data must be limited to only what is reasonably required to deliver a promised product, feature or service to a child.

3. Parental Control of Children's Data
   Parents, not the operator, should remain in control of data collected from the child. Providing parents with notice, choice and consent over whether or not their child's personal data is collected, and whether or not it is used or disclosed, should be maintained at all times while an operator intends to collect data from a child or is in possession of a child's data. This includes providing parents with a reasonable means to review the specific data or categories of data that may have been collected from their child, to request that it be deleted, and to request that the operator of the website or online service not collect data from their child in the future.

4. Security
   Operators must take reasonable measures to secure and maintain the confidentiality, security and integrity of data. Such measures must also include practices for regularly deleting data within a reasonable time frame after it is no longer needed.

5. Education
   Operators should maintain a baseline level of knowledge of privacy requirements and best practices. Regular assessments of policies and practices, as well as training of all employees on regulatory and company requirements in these areas should be a part of the responsibility accepted by an operator creating products intended for children.

B. Initial Engagement

Companies wishing to participate in iKeepSafe's Safe Harbor program (Member Companies) will begin their engagement with a discussion of the current stage of development, scope of product, existing practices and level of fluency with applicable regulation and industry best practices. This information will be used to gauge the level of guidance a particular company may require throughout the seal acquisition process.

Companies with products that are still in the concept or early-stage design phase will be provided with consultation and advice throughout the development process to ensure that final production results in a compliant product, eligible for the iKeepSafe Safe Harbor seal.

C. Required Materials

All companies will be required to provide the following documentation for review:

- Completed iKeepSafe Privacy Questionnaire and Data Table, which documents third party partners, links and plug-ins, and data collection, sharing, use and security practices and policies (Exhibit III, Appendix A)
- Copy of any existing privacy policy and terms of service
- Copy of any existing contractual agreements if company contracts directly with educational institutions
- Copy of any existing notices sent to parents requesting consent for data collection, use and/or disclosure
- Copy of any existing processes related to a parent's request to review or have deleted their child's data
- Copy of any existing policies and practices related to assessment of third party service providers and results of any such assessments
- Copy of written information security program

D. Technical Assessment

A technical analysis, conducted with an intercepting web proxy and network analyzer, will be made available to companies as needed to reveal the complete list of third parties receiving data from the product, the nature of that data, and how it is transmitted. (See Technological Capabilities and Mechanisms for Assessment below.) The capture files and reports will be archived for a period of 3 years, unless another time period is designated by the FTC.

E. Manual Assessment

All products will undergo a detailed and thorough manual review, with assessment of the complete product, along with the iKeepSafe Privacy Questionnaire and Data Table, any technical analysis results, privacy policy, notices sent to parents, processes related to a parent's request to review or have deleted their child's data, policies, practices and results of any third party assessments, and the written information security program. Elements that diverge from iKeepSafe Safe Harbor program guidelines or inconsistencies between what was divulged in the documentation and the actual product will be noted in a Compliance Report submitted to the Member Company, along with required changes.

All Member Companies will be provided with guidance on solutions to issues and consultation on implementation of solutions as needed.

Companies will be required to attest to having made the required changes. A final manual assessment will then be conducted to ensure that the product is in compliance.

F. Privacy Policy and Notice Development

Any existing privacy policies and notices will be reviewed as part of the manual assessment. However, for operators that do not yet have a privacy

policy or notices, the iKeepSafe Safe Harbor program will be available to create customized drafts. The drafts will generally be created after the Member Company has agreed to implementation of any required changes to its website or service, to ensure that the final policy and notices reflect practices that will exist in the final product. iKeepSafe Safe Harbor program will also assist as needed in developing other required policies and practices around compliance with the program.

G. Ongoing Assessment

At various times, but no less than three times per year of membership, Member Company products will be seeded for evaluation. Issues that arise will be brought to the Member Company's attention via a Notice of Concern memo (Exhibit III, Appendix B). Member Companies must respond to the Notice of Concern within five (5) business days in accordance with processes outlined in the Full Guidelines (Exhibit III). An aggregated summary of Notice of Concern issues and resolutions will be included in iKeepSafe Safe Harbor program annual reporting to the FTC per section 312.11(d)(1).

H. Renewals

Seals will be deemed to be renewable on an annual basis through a process of re-assessment. Thirty (30) days prior to the end of the calendar year of certification, Member Companies will be required to submit a new iKeepSafe Privacy Questionnaire and Data Table, a list of product updates, as well as assurances that they have assessed data handling practices of any third parties involved with the website or online service and conducted annual privacy training. These documents will be reviewed in conjunction with a manual review of the product and privacy policy to ensure that compliance has been maintained. Operators who remain in compliance will be allowed to renew their membership in the program. Any noted issues will be addressed via the Notice of Concern memo and process.

Technological Capabilities and Mechanisms for Assessment

The iKeepSafe Safe Harbor program intends to use a combination of manual and technical assessments to determine fitness of Member Companies to participate in and maintain good standing in the program.

Member Company products will be assessed and the guidelines enforced by iKeepSafe.

For Member Companies that do not have adequate visibility into third-party calls onto their products and services, the iKeepSafe Safe Harbor program may require that an HTTP and SSL proxy analysis be conducted to record network traffic, track the use and propagation of persistent identifiers, examine local storage, and otherwise assess the behavior of websites and online services. iKeepSafe Safe Harbor program will provide an authorized resource for such analysis if needed by a Member Company.

iKeepSafe Safe Harbor Program Business Model/Financials

iKeepSafe is a 501(c)3 nonprofit, established in 2005. Since that time iKeepSafe has maintained support for its initiatives through corporate sponsors, private foundations and public funds including Department of Education, Department of Justice and state specific grants focused on child online safety (from Utah, Virginia, Idaho and others).

iKeepSafe has been awarded grants from over thirty private foundations, including Sorenson Legacy Foundation, Eccles Foundation, and Silicon Valley Foundation. iKeepSafe does accept donations from corporate sponsors, however those corporations are not allowed to sit on iKeepSafe's board of directors.

iKeepSafe's roster of corporate sponsors, public funders and foundation supporters, along with funding from private donations, has helped to maintain the organization for the past nine years.

iKeepSafe's cash budget ranges between ---------- and ---------- with in-kind donations averaging an additional --------- per year.

Leadership is provided by Holly Hawkins (President and CEO), supported by a staff of 4 team members providing the following services: Vice President of Operations, Director of Policy and Communications, Director of Content Developer, and Administrative Manager.

The iKeepSafe Safe Harbor program has a standard pricing model per COPPA Safe Harbor assessment. iKeepSafe may provide discounted pricing to Member Companies that wish to take advantage of additional seals and services that iKeepSafe provides around privacy and may offer discounted pricing to smaller companies on an as-needed basis and at the sole determination of iKeepSafe.

The financial projections for the program are as follows.

EXHIBIT III
(Per § 312.11(b)(1-3), (c)(2) and (4), (d)(1-3))

iKeepSafe Safe Harbor Program Guidelines
iKeepSafe takes seriously the obligations of the industry community to afford strong privacy protections to children under the age of 13. In order to qualify for the iKeepSafe Safe Harbor program seal and maintain membership in the iKeepSafe Safe Harbor program, all Member Company operators of websites or online services that are in whole or in part directed or targeted to children, and which collect or maintain personal information from children are required to comply with the Children's Online Privacy Protection Rule (Part 312 of Title 16 of the CFR) and the following guidelines.

Determining the Target Audience:
In determining whether or not a website or online service is directed to children under 13, the iKeepSafe Safe Harbor program will consider all of the following factors:

- subject matter
- visual content
- use of animated characters
- presence of child-oriented activities and promotions
- music or other audio content
- age of models
- presence of child celebrities or celebrities who appeal to children
- language or other characteristics
- advertising promoting or appearing on the website or online service that is directed to children or otherwise indicating that the product is intended for children
- competent and reliable empirical evidence on the audience composition

No one of these factors will predominate over another, but instead the iKeepSafe Safe Harbor program will consider the totality of circumstances and factors when assessing whether or not a website or online service is directed to children.

The Member Company product will also be deemed directed to children if the Member Company or the iKeepSafe Safe Harbor Program has actual knowledge that information from children is being collected, used or disclosed.

Children as a Primary Target:
If a website or online service is directed to children under 13, and those children are the primary audience, the Member Company must assume that all visitors are children under the age of 13 and comply with all provisions of these guidelines for all users.

Children as a Secondary Target:
If a website or online service is directed to children under 13, but children are not the primary audience, the Member Company may ask users for their age via use of a neutral age-screening mechanism prior to the collection of personal information. Neutral age- screening mechanisms must allow users to freely choose an age or date of birth from a menu. Choices may not be limited to ages or dates that would

indicate that a user is over 13, and may not include any copy or visuals that suggest to the user how old they might need to be in order to move beyond the age gate. Session cookies or other technology should be employed to prevent users from easily changing their age or date of birth once submitted.

Personal information may not be collected prior to requesting the user's age, and in the case of users under the age of 13, it may not be collected, used or disclosed without prior parental consent as detailed in these guidelines. In addition, care should also be taken to ensure that users under 13 are allowed to participate in the site or service, and are not precluded from doing so based on their age.

General Audience:
A child-directed section of a website or online service that is otherwise intended for a general audience must also comply with these guidelines.

Definitions:
Child: an individual under the age of 13.

Collects or *collection:* gathering any personal information from a child by any means, including but not limited to:

- Requesting, prompting, or encouraging a child to submit personal information online, including, but not limited to, offering native sharing features that automatically open the user's email, IM, social networks or other communication features;
- Enabling a child to make personal information publicly available, such as in a chat room, message board, ecard or other public forum, in identifiable form. (If an operator takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records, it shall not be considered to have collected personal information in this situation); or
- Passive tracking of a child online.

Delete: to remove personal information so that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

Disclose or disclosure (with respect to personal information):

- Release of personal information collected by an operator from a child in identifiable form for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the website or online service as defined below; and
- Making personal information collected by an operator from a child publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a website or online service; a pen pal service; an email service; a message board; or a chat room.

Internet: collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

Online contact information: an email address or any other substantially similar identifier that permits direct contact with a person online, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.

Operator: any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, or offers products or services for sale through that website or online service, where such website or online service is operated:

- Among the several States or with 1 or more foreign nations;
- In any territory of the United States or in the District of Columbia, or between any such territory and
- Another such territory, or (2) Any State or foreign nation; or
- Between the District of Columbia and any State, territory, or foreign nation.

Any nonprofit operators wishing to become Member Companies must comply with all provisions of these guidelines.

Personal information is *collected or maintained on behalf of* an operator when: (a) it is collected or maintained by an agent or service provider of the operator; or (b) the operator benefits by allowing another person to collect personal information directly from users of such website or online service.

Parent includes a legal guardian.

Personal information: individually identifiable information about an individual collected online, including:

- A first and last name;
- A home or other physical address including street name and name of a city or town;
- Online contact information as defined in this section;
- A screen or user name where it functions in the same manner as online contact information, as defined in this section;
- A telephone number;
- A Social Security number;
- A persistent identifier that can be used to recognize a user over time and across different websites or online services. Persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;
- A photograph, video, or audio file where such file contains a child's image or voice;
- Geolocation information sufficient to identify street name and name of a city or town, including geolocation metadata associated with photos, videos or other user submissions; or
- Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Release of personal information: sharing, selling, renting, or transfer of personal information to any third party.

Support for the internal operations of the website or online service: activities necessary to:

- maintain or analyze the functioning of the website or online service;
- perform network communications;
- authenticate users of, or personalize the content on, the website or online service;
- serve contextual advertising on the website or online service or cap the frequency of advertising;
- protect the security or integrity of the user, website, or online service;
- ensure legal or regulatory compliance; or
- fulfill a request of a child as permitted by COPPA §§ 312.5(c)(3) and (4); so long as the information collected for the activities listed above is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose.

Third party: any person who is not:

- An operator with respect to the collection or maintenance of personal information on the website or online service; or
- A person who provides support for the internal operations of the website or online service and who does not use or disclose information protected under this part for any other purpose.

Obtaining verifiable consent: making reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

- Receives notice of the operator's personal information collection, use, and disclosure practices; and
- Authorizes any collection, use, and/or disclosure of the personal information.

REQUIREMENTS

1. Transparency

Clearly written policies explaining what data a website or online service collects from users, how such data is used, stored and to whom it may be disclosed are mandatory. Such policies must accurately reflect actual website or service data handling practices, and must be easy for the user to find and understand.

A. Privacy Policy:

Member Companies that collect or allow for the collection of personal information from children through their website or online service, must post a Privacy Policy that explains their data collection, use, disclosure, security and deletion practices.

i. Content:

The Privacy Policy must contain the following information:

(a) Name, address, telephone number and email address of all operators collecting or maintaining personal information from children
   - Note: The policy may include the name, address, phone number and email address of one operator who will respond to all inquiries from parents about the different operators' privacy policies and use of children's information as long as the names of all operators collecting or maintaining personal information from children are also listed in the policy

(b) Description of what personal and non-personal information is collected from users, including:
   - whether or not the website or online service allows or encourages a child to make personal information publicly available, and how that might be done
   - an explanation of how the information is used by the operator
   - whether or not any of the information is disclosed to third parties or partners, including what information might be disclosed and why
   - that a parent has the right to review, have deleted and/or refuse to permit further collection or use of the child's information, along with information on how to do so
   - consequences or implications for a user refusing collection of data

(c) A statement explaining the operator's general practices related to data security and integrity

(d) Information on how consumers can ask questions or file complaints related to the privacy policy and practices, and a link to the iKeepSafe Safe Harbor program dedicated consumer complaint email address

ii. Placement and Appearance:
A clear, prominent link to the privacy policy must be placed on the home or landing page of the website or online service and at each area of the product where personal information is collected from children. The link must appear in close proximity to the area where personal information is requested.

(a) It may be acceptable to place the link in the footer of the website or online service. In these cases, the link must be clearly highlighted and set apart from other links in the footer, with clear and contrasting color and larger typeface.

(b) An operator of a general audience website or online service that contains a children's area must post a link to a privacy policy detailing data collection and handling practices related to children on the home or landing page of that children's area.

(c) With respect to mobile apps, in addition to the placements noted above, a link to the privacy policy must be posted at the point of purchase.

(d) For all products supplied directly to schools, a copy of the privacy policy must be available to the school prior to completion of the sale, download or installation of the product.

2. Minimization of Data Collection

In the arena of product development, media and marketing intended for children, collection of data should be limited to only what is reasonably required to deliver a promised product, feature or service to a child user and to what is reasonably needed to maintain and further develop the website or service.

A. Limitations on Collection of Data

Member Companies may only collect 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. Collection of more data than is reasonably necessary to provide features, activities or support for internal operations is not acceptable. Data collection practices will be assessed via the iKeepSafe Privacy Questionnaire and Data Table, manual assessment and technical analysis.

Collection of all personal information must comply with the parental notice and consent requirements outlined below, and all data collection and handling practices must be disclosed in the privacy policy.

3. Parental Control of Children's Data

Parents should remain in control of data collected from their child. Providing parents with notice, choice and consent over whether or not their child's data is collected, and whether or not it is used or disclosed, should be maintained at all times while an operator intends to collect data from a child or is in possession of a child's data. This includes providing parents with a reasonable means to review the specific data or categories of data that may have been collected from their child, allowing them to request that it be deleted, and/or that the operator not collect any further data from the child. As noted above, information about how parents might take advantage of this option must be included in the privacy policy.

Member Companies should have a process in place that takes into account available technology to provide for verification that the person requesting to review the data is the parent.

A. Prior Consent for Data Collection

Operators must obtain verifiable parental consent before collecting, using and/or disclosing personal information from children. Operators must also provide parents with notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.

In addition, Member Companies must give the parent the option to consent to the collection and use of the child's personal information without agreeing to disclosure of the child's personal information to third parties.

i. Consent from Schools

Member Companies contracting directly with a school 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.

(a) Providing such consent in lieu of the parent is at the sole discretion of the school.

(b) If the Member Company intends to use or disclose students' personal information for other commercial purposes, it must obtain prior consent directly from the parents as detailed below

B. Methods for Obtaining Parental Consent

Member Companies must use one of the methods described below to verify that the person providing consent is the parent:

(a) Provide parents with a consent form to be signed and returned via mail, facsimile or electronic scan

(b) Require that the parent provide a credit card, debit card or other online payment system that provides notification of each discrete transaction, and use it in connection with a monetary transaction

(c) Provide a toll-free number or video conference system staffed by personnel who have been trained to identify whether or not the caller is a parent

(d) Check a parent's form of government-issued ID against databases of such information. (The ID must be deleted from the Member Company's records promptly after such verification is complete.)

(e) Knowledge-based authentication, as long as the specific process uses dynamic, multiple-choice questions with enough options to ensure that the chances of a child guessing the correct answers is low and the questions used are of sufficient difficulty that it would be difficult for a child in the household to figure out the answers

(f) Where a child's personal information is collected but not disclosed, an operator may send an email to the parent requesting prior consent for the collection of personal information, provided that the email is followed up after receipt of consent with one of the following:

- A confirmation email, letter or telephone call to the parent confirming the parent's consent, if such information has been received from the parent
  - Such follow-up must advise parents that they may revoke their prior consent if they choose to

i. Alternate Methods for Obtaining Parental Consent

Member Companies may propose additional methods for obtaining verifiable parental consent. Such proposals must include full details of the process envisioned, including what data will be captured, how it will be handled and who at the Member Company will be responsible for executing the process. Any such proposed method must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.

Proposals will be evaluated by the iKeepSafe Safe Harbor program to determine whether or not the methods meet these stated requirements and will be considered acceptable under the iKeepSafe Safe Harbor program. Any such approval will be at iKeepSafe Safe Harbor program's discretion, based on whether or not it determines that the proposed method complies with requirements of the Children's Online Privacy Protection Act and these guidelines.

ii. Exceptions to Obtaining Prior Parental Consent:

In certain use cases as described below, prior parental consent is not required:

- When the only purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent
    - The information must be deleted from the operator's records if parental consent is not received after a reasonable time

- When the purpose of collecting a parent's online contact information is to provide voluntary notice to, and update the parent about, the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information.
    - In these cases, the parent's online contact information may not be used for any other purpose
    - Reasonable efforts, taking into account available technology, must be taken to ensure that the person receiving the notice is the parent

- When the only purpose of collecting online contact information from a child is to respond once to a specific request from a child.
    - The information may not be disclosed or used for any other purpose, including to contact the child more than once
    - The information must be deleted from the Member Company's records promptly after responding to the child's request

- When the purpose of collecting a child's and a parent's online contact information is to respond directly, more than once, to a child's specific request, such as when a child requests to sign up for an operator's newsletter.
    - The information may not be used for any other purpose, and may not be disclosed or combined with any other information collected from the child
    - Although prior consent is not required for the first response to the child, Member Companies must provide parents with notice of the information that was collected, what it is being used for, that parents may opt their child out of further contact and how to do so, all prior to the second contact with the child.

- When the purpose of collecting a child's name and online contact information is to:
    - Protect the security and/or integrity of its website or online service
    - Take precautions against liability
    - Respond to a judicial process
    - Provide information to law enforcement agencies or for an investigation on a matter related to public safety to the extent permitted by law and where such information is not being used for any other purpose

- When a persistent identifier is collected by an operator *for the sole purpose of providing support for internal operations* (as defined above) for their website or online service.

C. Content of the Notice for Parental Consent

Member Companies must provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. The notice must be clearly and understandably written, complete, and must not contain any unrelated, confusing, or contradictory materials. The notice may contain an optional, brief statement explaining what the website or online service is. However, it may not contain marketing, sell or other promotional language.

In all cases, it must be clear that a parent may agree to allow for the collection and use of a child's personal information without agreeing to the disclosure of that information to third parties, unless both are required in order to deliver a particular website or online service feature and the parent would like the child to be able to participate in that feature.

There are different requirements for the content of the notice requesting parental consent, depending on the use case:

(a) Request for Consent to Collect, Use or Disclose a Child's Personal Information:
- This notification must include the following:
  - That the operator has collected the parent's online contact information from the child, and, if applicable, the name of the child or the parent, in order to obtain the parent's consent;
  - That the parent's consent is required for the collection, use, or disclosure of the information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide consent;
  - Any additional items of personal information the operator intends to collect from the child, and/or potential opportunities for the disclosure of personal information, should the parent provide consent;
  - How the parent can provide consent for the collection, use, and disclosure of the information; and
  - That if the parent does not provide consent within a reasonable time from the date the notice was sent, the operator will delete the parent's online contact information from its records.
  - A hyperlink to the Privacy Policy

(b) Voluntary Notice of a Child's Online Activities Not Involving Collection, Use or Disclosure of Personal Information
- This notice is optional, but when provided it must include the following:
  - That the operator has collected the parent's online contact information from the child to provide notice to, and update the parent about, a child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information;
  - That the parent's online contact information will not be used or disclosed for any other purpose;
  - That the parent may refuse to permit the child's participation in the website or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and
  - A hyperlink to the Privacy Policy

(c) Notice of Intent for Multiple Contact
- This notice must include the following:
  - That the operator has collected the child's online contact information from the child to communicate with the child more

than once;

- That the operator has collected the parent's online contact information to notify the parent that the child has registered to receive multiple online communications from the operator;

- That the online contact information collected from the child will not be used for any other purpose, and that it will not be disclosed, or combined with any other information collected from the child;
- That the parent may refuse to permit further contact with the child and require the deletion of the parent's and child's online contact information, and how the parent can do so;
- That if the parent fails to respond to the notice, the operator may use the online contact information collected from the child for the stated purpose; and
- A hyperlink to the Privacy Policy

(d) Notice to Protect Safety
- This notice must include the following:
  - That the operator has collected the name and the online contact information of the child and the parent in order to protect the safety of the child;
  - That the information will not be used or disclosed for any other purpose;
  - That the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so;
  - That if the parent fails to respond to the notice, the operator may use the information for the stated purpose; and
  - A hyperlink to the Privacy Policy

4. Security

Operators must take responsibility for safeguarding data collected from or about their users. Reasonable measures must be taken to secure and maintain the confidentiality and integrity of data. Such measures must also include practices for regularly deleting data within a reasonable time frame after it is no longer being used or is no longer needed.

A. Data Security, Confidentiality and Integrity

Data must be stored securely, with sensitive data, such as personal information, stored separately from other data.

i. Access to data must be limited to authorized employees, and a procedure must be in place to revoke access when an employee leaves the organization.

ii. Inactive data must be purged on a regular basis, with a defined process in place for deleting and destroying said data.

iii. A defined process must also be in place for deleting and destroying data when requested by a parent
- This process must include steps to confirm that the person requesting review or deletion of a child's data is the parent

iv. A defined process must exist for conducting regular security audits.

B. Third Party Service Providers

Member Companies must establish procedures and practices for:

- informing any third party service providers that its site or online service is directed to children
- informing any third party service providers of its data privacy and security policies and practices
- receiving written assurances that any third party service providers are able to comply with those policies and practices

i. Third Party Assessment Requirements

Member Companies must assess the privacy policies and practices of any third party service providers to ensure that they are capable of complying with Member Company's policies and practices, including those related to the collection, use, transfer, confidentiality, security and integrity of user data.

(a) Member Companies must receive affirmative assurances from third parties to that effect

(b) Such procedures, assessments and assurances related to third party service providers must be repeated on an annual basis, at any time at which Member Company's policies or practices change, and at any time that they are made aware of changes to a third party provider's policies or practices. Any such changes must also be reported to iKeepSafe Safe Harbor program for assessment.

(c) Certification that these requirements have been met must be submitted to iKeepSafe Safe Harbor program as part of the initial certification and annual renewal process.

5. Education

Operators should maintain baseline knowledge of privacy requirements and best practices. Regular assessments of policies and practices, as well as training of all employees on iKeepSafe Safe Harbor program requirements in these areas should be a part of the responsibility accepted by Member Companies.

A. Training:

Member Companies are required to provide privacy training to all company employees responsible in whole or in part for design, production, development, operations and marketing of their products. Such training should include all employees who are directly or peripherally involved in collection, use, storage, disclosure or any other handling of data. Training is required to be conducted a minimum of one time per year. Training will be provided by an iKeepSafe Safe Harbor program representative if requested.

Certification that such training has been conducted must be submitted to iKeepSafe Safe Harbor program as part of the annual renewal process.

6. Disciplinary Action (Per § 312.11(b)(3) and § 312.11(c)(4)(ii))

iKeepSafe Safe Harbor program takes seriously its obligations and responsibilities in providing this program to Member Companies. As such, any of the following may be considered grounds, in the iKeepSafe Safe Harbor program's sole discretion, for revocation of a Member Company's iKeepSafe Safe Harbor seal:

- Willful or repeated noncompliance with any of the guidelines
- Failure to cooperate with iKeepSafe Safe Harbor program requests for product changes to meet requirements of these guidelines
- Intentional misstatements in any communications related to Member Company's products, services or materials used for

assessment
- Failure to report consumer complaints
- Failure to respond to consumer complaints as described below Member Companies whose seal has been revoked will be

reported to the FTC.

Descriptions of all disciplinary action will be included in iKeepSafe Safe Harbor program's annual report to the FTC.

A. Complaints:
Member Companies must keep a record of all complaints that it receives in relation to privacy and data handling practices or compliance with these guidelines.

i. Member Company must submit any such complaints to the iKeepSafe Safe Harbor program upon receipt

ii. Within 5 business days of receiving such a complaint, Member Company must submit a letter to the iKeepSafe Safe Harbor Seal program explaining its intent to resolve the concern, including, if applicable, product adjustments to ensure continued compliance with iKeepSafe Safe Harbor program guidelines and any voluntary consumer redress.

The letter must include one of the following:

(a) An explanation of how the Member Company intends to rectify the complaint (including, but not limited to product adjustments and consumer redress), anticipated time frame needed to do so, and confirmation that any data that may have been collected in relation to the complaint not in compliance with the iKeepSafe Safe Harbor program guidelines will be deleted promptly from its records
   - Any such plan for resolution must be approved by the iKeepSafe Safe Harbor program; such approval to be provided within 5 business days

(b) A request for assistance from the iKeepSafe Safe Harbor program on addressing concerns referenced in the complaint

(c) A request for review by iKeepSafe Safe Harbor program on the validity of the complaint, if there is concern on the part of the Member Company that the complaint is without merit in whole or in part

iii. Decisions made by iKeepSafe Safe Harbor program regarding validity of complaints and/or product changes and consumer redress needed in response to complaints shall be deemed to be binding on the Member Company. All product changes made in response to complaints will be reviewed by iKeepSafe Safe Harbor program in order to certify compliance with these guidelines.

In addition, iKeepSafe will provide a dedicated email address, promoted in a dedicated section on the iKeepSafe website, by which consumers may send complaints directly to the iKeepSafe Safe Harbor program. This email address must also be disclosed in the Member Company's privacy policy. iKeepSafe Safe Harbor program will notify Member Company upon receipt of any such complaints and will require a response as noted above.

In all cases, the iKeepSafe Safe Harbor program will also conduct its own assessment of any feature of a Member Company website or online service that is the subject of a complaint in order to determine its perspective on validity of the complaint and appropriate steps for correction of the issues, as well as any additional enforcement steps that it deems appropriate as noted below.

Member Companies will be required to respond to consumers explaining the resolution of their complaint. Each response will include information

about how to contact the Member Company and/or iKeepSafe Safe Harbor program to appeal the resolution if the consumer finds it to be unsatisfactory.

B. Enforcement

Member Companies that receive multiple complaints may also be subject to:

- Anonymous payments to the United States Treasury
- Consumer redress (in addition to the required deletion of data, if applicable)
- Revocation of the iKeepSafe Safe Harbor program seal and referral to the FTC

PROCESS:

A. Initial Certification:

Companies interested in participating in the iKeepSafe Safe Harbor program will begin their engagement with a call with iKeepSafe's Compliance Advisor to discuss the current stage of development, scope of product, existing practices and level of fluency with applicable regulation and industry best practices. Companies will also be required to complete and return the Data iKeepSafe Privacy Questionnaire and Data Table (Appendix A).

The iKeepSafe Privacy Questionnaire and Data Table must be submitted by an authorized representative of the Member Company, who will be asked to attest to the truthfulness and accuracy of the information. Member Companies understand that the iKeepSafe Safe Harbor program will use representations within the documents in part to assess Member Company's compliance with the program's safe harbor provisions for the Children's Online Privacy Protection Act.

In addition to the completed iKeepSafe Privacy Questionnaire and Data Table, Member Companies will also be required to submit the following documents

- Copy of any existing privacy policy
- Copy of any existing notices sent to parents requesting consent for data collection, use and/or disclosure
- Copy of any existing processes related to a parent's request to review and/or have deleted their child's data
- Copy of any existing policies and practices related to assessment of third party service providers
- Copy of written information security program

As needed, iKeepSafe Safe Harbor program will require that Member Companies conduct a technical analysis of any existing products. An authorized resource will be provided to conduct the analysis, if needed.

The Compliance Advisor to the iKeepSafe Safe Harbor program will review the product, along with all submitted documentation and the results of any technical analysis. Upon completion of the review, the Member Company will be provided with a detailed report outlining any features, practices, policies, notices or other elements that are not deemed to be in compliance with iKeepSafe Safe Harbor program guidelines, along with required changes. Assistance in drafting policies, practices and notices will also be provided as needed.

Once changes have been completed, iKeepSafe Safe Harbor program Compliance Advisor will assess the changes and if the product is deemed to be in compliance, the iKeepSafe Safe Harbor Program Seal will be provided for use on the company product.

B. Reassessments and Bi-Annual Reports:

At various points throughout the year of membership, but no less than three, iKeepSafe Safe Harbor program will, at a time of its choosing, revisit each Member Company product and reassess practices. If elements of the product are deemed to no longer be in compliance, or if new elements have been added that are not deemed to be in compliance, iKeepSafe Safe Harbor program will submit a Notice of Concern Memo (Appendix B) to the Member Company, along with required changes.

Member Companies will have five (5) business days to respond in writing to the Notice of Concern and attest that the required changes will be made in a specific and timely fashion. Member Companies will be provided with a certification form to sign and submit to iKeepSafe Safe Harbor program attesting to completion of the changes.

Failure to respond to the Notice of Concern within the allotted time frame, or failure to complete the changes in a timely fashion may, at iKeepSafe Safe Harbor program's sole discretion, result in disciplinary action as described above.

To ensure transparency and encourage ongoing compliance, each Member Company will receive reports providing the results of iKeepSafe Safe Harbor program's reassessments of its product(s).

C. Annual Review and Reporting

On an annual basis, iKeepSafe Safe Harbor program will conduct a full reassessment of all Member Company products and compliance with the iKeepSafe Safe Harbor program guidelines. As part of the reassessment, Member Companies will be required to submit a new iKeepSafe Privacy Questionnaire and Data Table, a list of any product updates, and assurances that data handling practices of any third parties involved with the website or online service have been assessed, and annual privacy training has been completed.

If products are deemed to no longer be in compliance, iKeepSafe Safe Harbor program will submit a Notice of Concern to the relevant Member Company, along with the required changes. Member Companies will have five (5) business days to respond in writing to the Notice of Concern and attest that the required changes will be made in a specific and timely fashion.
Member Companies will be provided with a certification form to sign and submit to iKeepSafe Safe Harbor program attesting to completion of the changes.

iKeepSafe Safe Harbor program will use the results of its Member Company reassessments and bi-annual reports to create aggregated, summary reporting on Member Company compliance to be submitted to the Federal Trade Commission on an annual basis. Reporting will include:

(a) Details on assessments and reassessments conducted by iKeepSafe Safe Harbor program's Compliance Advisor for each Member Company
(b) Number and general nature of consumer complaints filed against Member Companies
(c) Aggregated summary of issues that, as of the date of the report remain unresolved, and expected resolutions
(d) Aggregated summary of changes made throughout the year to correct any compliance issues
(e) Description of disciplinary action taken and any instances in which seals have been revoked

Reports will be maintained on file with the iKeepSafe Safe Harbor Program for a minimum of 3 years.

D. Company Visits

Member Companies may request on-site visits to provide the following:

- Education and staff training
- Consultation on application of the guidelines or implementation of changes (also available by phone and email)

On-site visits to be at the sole expense of the requesting Member Company.

E. Member Company Obligations: Member Companies shall be required to:

- Designate one representative who shall serve as the point of contact for iKeepSafe Safe Harbor program, and who shall be authorized by the company to manage communications and initiate changes to products as needed
- Notify iKeepSafe Safe Harbor program of any material changes to the product, including changes to features, privacy policy, notices or data security practices, promotions or third party partners, or other changes that may impact data practices.
    - All such changes will be reviewed by the iKeepSafe Safe Harbor program Compliance Advisor
- Provide a new iKeepSafe Privacy Questionnaire and Data Tablewithin thirty (30) days of their anniversary date for use in the iKeepSafe Safe Harbor program annual review
- Provide certification that privacy training and assessment of third parties has been conducted within thirty (30) days of their anniversary date for use in the iKeepSafe Safe Harbor program annual review
- Provide iKeepSafe Safe Harbor program with written notice within 30 days if Member Company changes its name, sells or otherwise transfers products covered under the seal program to another party or changes the URL or name of any website or online service covered by the seal program

APPENDIX A:

iKeepSafe Privacy Questionnaire and Data Table

iKeepSafe Privacy Questionnaire

<insert vendor name>

A. General

1. [redacted]

2. [redacted]

3. Check all that apply:

	[redacted]
	[redacted]
	[redacted]
	[redacted]
	[redacted]

B. Data Collection & Use

1. [redacted]

2. [redacted]

3. [redacted]

[redacted]

4. [redacted]

5. [redacted]

6. [redacted]

7. [redacted]

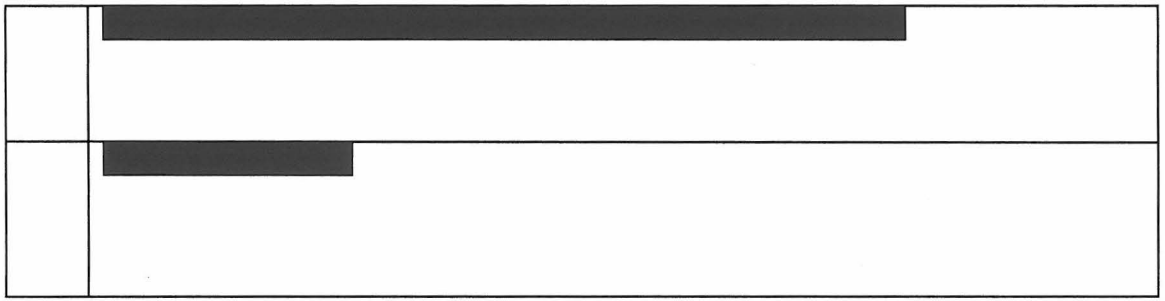
8. [redacted]

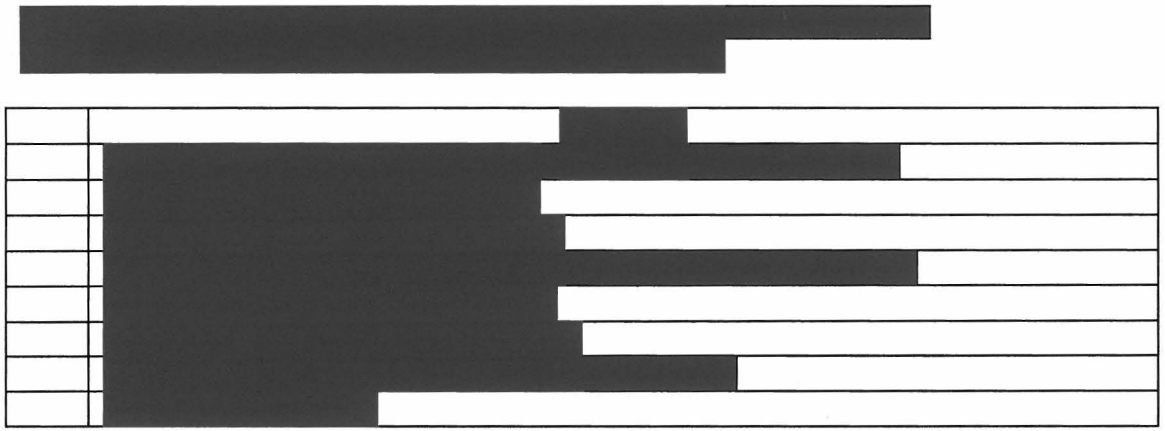
[redacted]

C. Interactivity

[redacted]

1. [redacted]





3. [redacted]

4. [redacted]

5. [redacted]

6. [redacted]

D. Third Party Service Providers

1. [redacted]

2. [redacted]

3. [redacted]

4. [redacted]

E. Data Sharing

1. [redacted]

F. Data Security

1. [redacted]

2. [redacted]

3. [redacted]

[redacted]

5. [redacted]

6. [redacted]

7. [redacted]

8. [redacted]

9. [redacted]

G. Data Retention and Deletion

1. [redacted]

2. [redacted]

3. [redacted]

4. [redacted]

H. Security Controls and Audits

[redacted]

	[redacted]	

2. [redacted]

3. [redacted]

4. [redacted]

5. [redacted]

6. [redacted]

7. [redacted]

8. [redacted]

9. [redacted]

10. [redacted]

I. Compliance Training

1. [redacted]

[redacted]

2. [redacted]

[redacted]

I. Additional Information

[redacted]

[redacted]

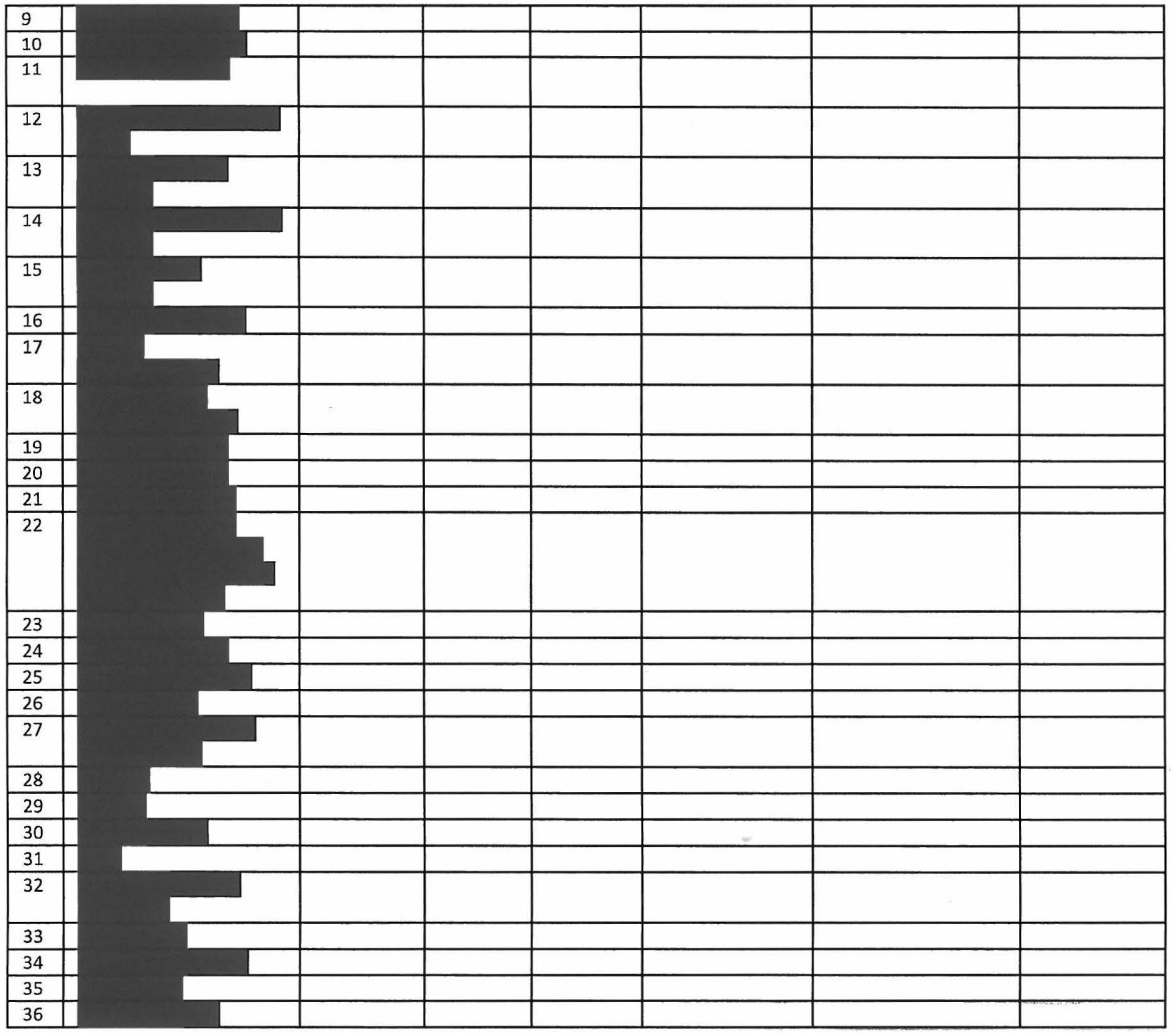
[redacted]

iKeepSafe Vendor Data Table

<insert client name>

DATA TABLE

#	[redacted]						
1							
2							
3							
4							
5							
6							
7							
8							



APPENDIX B
Notice of Concern Memo

Date:
Company Contact:

The results of an examination of _[product]__ have revealed the following concerns, which indicate that your product is not currently in compliance with the iKeepSafe Safe Harbor program requirements:

—
—
—
—

In order to maintain membership in the iKeepSafe Safe Harbor program and continue displaying the iKeepSafe Safe Harbor program marks on your product, please make the following changes. Changes must be made promptly.

—
—
—
—

Please sign and return a copy of this Notice of Concern within five (5) business days of receipt to indicate: (1) your acknowledgement of the issues; and (2) your acknowledgement that failure to resolve the issues in a timely manner may jeopardize your continued use of the iKeepSafe Safe Harbor program marks. Please also indicate the anticipated time frame needed to resolve the issues: _

We remain available to consult with you and guide you through implementation of any requested changes. Please feel free to contact us to discuss your compliance needs, questions and concerns.

Thank you.

Signed and Acknowledged:

_____

Name: Company: Title: Date:

Exhibit IV
Chart Comparing Seal Requirements to COPPA Provisions
(Per § 312.11(c)(3))

Children's Online Privacy Protection Act	Corresponding iKeepSafe Safe Harbor Seal Program Provisions
§ 312.2 Definitions.	Exhibit III, Definitions

§ 312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. *General requirements*. It shall be unlawful for any operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting or maintaining personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under this part. Generally, under this part, an operator must: (a) Provide notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information (§ 312.4(b)); (b) Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children (§ 312.5); (c) Provide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance (§312.6); (d) 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 (§ 312.7); and (e) Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children (§ 312.8).	<u>Transparency</u> Clearly written policies explaining what data a website or online service collects from users, how such data is used, stored and to whom it may be disclosed are mandatory. Such policies must accurately reflect actual website or service data handling practices, and must be easy for the user to find and understand. <u>Privacy Policy</u>: Member Companies that collect or allow for the collection of personal information from children through their website or online service, must post a Privacy Policy that explains their data collection, use, disclosure, security and deletion practices. Content: The Privacy Policy must contain the following information: - Name, address, telephone number and email address of all operators collecting or maintaining personal information from children o Note: The policy may include the name, address, phone number and email address of one operator who will respond to all inquiries from parents about the different operators' privacy policies and use of children's information as long as the names of all operators collecting or maintaining personal information from children are also listed in the policy - Description of what personal and non-personal information the operator collects from users, including: o whether or not the website or online service allows or encourages a child to make personal information publicly available, and how that might be done

  - an explanation of how the information is used by the operator
  - whether or not any of the information is disclosed to third parties or partners, including what information might be disclosed and why
  - that a parent has the right to review, have deleted and/or refuse to permit further collection or use of the child's information, along with information on how to do so
  - consequences or implications for a user refusing collection of data
- A statement explaining the operator's general practices related to data security and integrity
- Information on how consumers can ask questions or file complaints related to the privacy policy and practices

Placement and Appearance:
A clear, prominent link to the privacy policy must be placed on the home or landing page of the website or online service and at each area of the product where personal information is collected from children. The link must appear in close proximity to the area where personal information is requested.

- It may be acceptable to place the link in the footer of the website or online service. In these cases, the link must be clearly highlighted and set apart from other links in the footer, with clear and contrasting color and larger typeface.
- An operator of a general audience website or online service that contains a children's area must post a link to a privacy policy detailing data collection and handling practices related to children on the home or landing page of that children's area.
- With respect to mobile apps, in addition to the placements noted above, a link to the privacy policy must be posted at

the point of purchase.

- For all products supplied directly to schools, a copy of the

privacy policy must be available to the school prior to completion of the sale, download or installation of the product.

Minimization of Data Collection

In the arena of product development, media and marketing intended for children, collection of data should be limited to only what is reasonably required to deliver a promised product, feature or service to a child user and to such data reasonably needed to maintain and further develop the website or service.

Limitations on Collection of Data

Member Companies may only collect 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. Collection of more data than is reasonably necessary to provide features, activities or support for internal operations is not acceptable.

Collection of all personal information must comply with the parental notice and consent requirements outlined above, and all such data collection and handling practices must be disclosed in the privacy policy.

Parental Control of Children's Data

Parents should remain in control of data collected from their child. Providing parents with notice, choice and consent over whether or not their child's data is collected, and whether or not it is used or disclosed, should be maintained at all times while an operator intends to collect data from a child or is in possession of a child's data. This includes providing parents with a reasonable means to review the specific data or categories of data that may have been collected from their child, allowing them to request that it be deleted, and/or that the operator not collect any further data from the child.

Member Companies should have a process in place that takes into

account available technology to provide for verification that the person requesting to review the data is the parent.

Prior Consent for Data Collection

Operators must obtain verifiable parental consent before collecting, using and/or disclosing personal information from children and must provide parents with notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.

In addition, Member Companies must give the parent the option to consent to the collection and use of the child's personal information without agreeing to disclosure of the child's personal information to third parties.

Consent from Schools

Member Companies contracting directly with a school 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.

- Providing such consent in lieu of the parent is at the sole discretion of the school.
- If the Member Company intends to use or disclose students' personal information for other commercial purposes, it must obtain prior consent directly from the parents

Methods for Obtaining Parental Consent

Member Companies must use one of the methods described below to verify that the person providing consent is the parent:

- Provide parents with a consent form to be signed and returned via postal mail, facsimile or electronic scan
- Require that the parent provide a credit card, debit

card or other online payment system that provides notification of each discrete transaction, and use it in

connection with a monetary transaction

- Provide a toll-free number or video conference system staffed by personnel who have been trained to identify whether or not the caller is a parent
- Check a parent's form of government-issued ID against databases of such information. (The ID must be deleted from the Member Company's records promptly after such verification is complete.)
- Knowledge-based authentication, as long as the specific process uses dynamic, multiple-choice questions with enough options to ensure that the chances of a child guessing the correct answers is low and the questions used are of sufficient difficulty that it would be difficult for a child in the household to figure out the answers
- Where a child's personal information is collected but not disclosed, an operator may send an email to the parent requesting prior consent for the collection of personal information, provided that the email is followed up after receipt of consent with one of the following:
    - A confirmation email, letter or telephone call to the parent confirming the parent's consent, if such information has been received from the parent
        - Such follow-up must advise parents that they may revoke their prior consent if they choose to

Exceptions to Obtaining Prior Parental Consent:
In certain use cases as described below, prior parental consent is not required:

- When the only purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent

- The information must be deleted from the

operator's records if parental consent is not received after a reasonable time

- When the purpose of collecting a parent's online contact information is to provide voluntary notice to, and update the parent about, the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information.
    - In these cases, the parent's online contact information may not be used for any other purpose
    - Reasonable efforts, taking into account available technology, must be taken to ensure that the person receiving the notice is the parent
- When the only purpose of collecting online contact information from a child is to respond once to a specific request from a child.
    - The information may not be disclosed or used for any other purpose, including to contact the child more than once
    - The information must be deleted from the Member Company's records promptly after responding to the child's request
- When the purpose of collecting a child's and a parent's online contact information is to respond directly, more than once, to a child's specific request, such as a request to sign up for an operator's newsletter.
    - The information may not be used for any other purpose, and may not be disclosed or combined with any other information collected from the child
    - Although prior consent is not required for the first response, Member Companies must

provide parents with notice of the information that was collected, what it is being used for,

that parents may opt their child out of further contact and how to do so, all prior to the second contact with the child. For requirements, see Content of the Notice for Parental Consent Section below.

- When the purpose of collecting a child's name and online contact information is to:
  - Protect the security and/or integrity of its website or online service
  - Take precautions against liability
  - Respond to a judicial process
  - Provide information to law enforcement agencies or for an investigation on a matter related to public safety to the extent permitted by law and where such information is not being used for any other purpose
- When a persistent identifier is collected *for the sole purpose of providing support for internal operations* (as defined above) for their website or online service.

Security

Operators must take responsibility for safeguarding data collected from or about their users. Reasonable measures must be taken to secure and maintain the confidentiality, security and integrity of data. Such measures must also include practices for regularly deleting data within a reasonable time frame after it is no longer being used or is no longer needed.

Data Security and Integrity

Data must be stored securely, with sensitive data, such as personal information, stored separately from other data.

- Access to data must be limited to authorized employees, and a procedure must be in place to revoke access when an employee leaves the organization.

- Inactive data must be purged on a regular basis, with a defined process in place for deleting and destroying

said data.
  - A defined process must also be in place for deleting and destroying data when requested by a parent
    - This process must include steps to confirm that the person requesting review or deletion of a child's data is the parent
  - A defined process must exist for conducting regular security audits.

Third Party Service Providers

Member Companies must establish procedures and practices for:

- informing any third party service providers that its site or online service is directed to children
- informing any third party service providers of its data privacy and security policies and practices
- receiving written assurances that any third party service providers are able to comply with those policies and practices

Third Party Assessment Requirements

Member Companies must assess the privacy policies and practices of any third party service providers to ensure that they are capable of complying with Member Company's policies and practices, including those related to the collection, use, transfer, confidentiality, security and integrity of user data.

- Member Companies must receive affirmative assurances from third parties to that effect
- Such procedures, assessments and assurances related to third party service providers must be repeated on an annual basis, at any time at which Member Company's policies or practices change, and at any time that they are made aware of changes in a third party provider's policies or practices. Any such changes must also be reported to iKeepSafe Safe

Harbor program for assessment.

	• Certification that these requirements have been met must be submitted to iKeepSafe Safe Harbor program as part of the initial certification and annual renewal process.

§ 312.4 Notice. (a) *General principles of notice.* It shall be the obligation of the operator to provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials. (b) *Direct notice to the parent.* An operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented. *(c) Content of the direct notice to the parent.* (1) *Content of the direct notice to the parent under § 312.5(c)(1) (Notice to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information).* This direct notice shall set forth: (i) That the operator has collected the parent's online contact information from the child, and, if such is the case, the name of the child or the parent, in order to obtain the parent's consent; (ii) That the parent's consent is required for the collection, use, or disclosure of such information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent; (iii) The additional items of personal information the operator intends to collect from the child, or the potential opportunities for the disclosure of personal information, should the parent provide consent; (iv) A hyperlink to the operator's online notice of its information practices required under § 312.4(d); (v) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and (vi) That if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the	<u>Transparency</u> Clearly written policies explaining what data a website or online service collects from users, how such data is used, stored and to whom it may be disclosed are mandatory. Such policies must accurately reflect actual website or service data handling practices, and must be easy for the user to find and understand. <u>Privacy Policy</u>: Member Companies that collect or allow for the collection of personal information from children through their website or online service, must post a Privacy Policy that explains their data collection, use, disclosure, security and deletion practices. Content: The Privacy Policy must contain the following information: • Name, address, telephone number and email address of all operators collecting or maintaining personal information from children o Note: The policy may include the name, address, phone number and email address of one operator who will respond to all inquiries from parents about the different operators' privacy policies and use of children's information as long as the names of all operators collecting or maintaining personal information from children are also listed in the policy • Description of what personal and non-personal information the operator collects from users, including: o whether or not the website or online service allows or encourages a child to make personal information publicly available, and how that might be done o an explanation of how the information is used by the operator

parent's online contact information from its records. (2) *Content of the direct notice to the parent under § 312.5(c)(2) (Voluntary Notice to Parent of a Child's Online Activities Not Involving the Collection, Use or Disclosure of Personal Information).* Where an operator chooses to notify a parent of a child's participation in a website or online service, and where such site or service does not collect any personal information other than the parent's online contact information, the direct notice shall set forth: (i) That the operator has collected the parent's online contact information from the child in order to provide notice to, and subsequently update the parent about, a child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information; (ii) That the parent's online contact information will not be used or disclosed for any other purpose; (iii) That the parent may refuse to permit the child's participation in the website or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and (iv) A hyperlink to the operator's online notice of its information practices required under § 312.4(d). (3) *Content of the direct notice to the parent under § 312.5(c)(4) (Notice to a Parent of Operator's Intent to Communicate with the Child Multiple Times).* This direct notice shall set forth: (i) That the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child; (ii) That the operator has collected the parent's online contact information from the child in order to notify the parent that the child has registered to receive multiple online communications from the operator; (iii) That the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child; (iv) That the	o whether or not any of the information is disclosed to third parties or partners, including what information might be disclosed and why o that a parent has the right to review, have deleted and/or refuse to permit further collection or use of the child's information, along with information on how to do so o consequences or implications for a user refusing collection of data • A statement explaining the operator's general practices related to data security and integrity • Information on how consumers can ask questions or file complaints related to the privacy policy and practices Placement and Appearance: A clear, prominent link to the privacy policy must be placed on the home or landing page of the website or online service and at each area of the product where personal information is collected from children. The link must appear in close proximity to the area where the personal information is requested. • It may be acceptable to place the link in the footer of the website or online service page. In these cases, the link must be clearly highlighted and set apart from other links in the footer, with clear and contrasting color and larger typeface. • An operator of a general audience website or online service that contains a children's area must post a link to a privacy policy detailing data collection and handling practices related to children on the home or landing page of that children's area. • With respect to mobile apps, in addition to the placements noted above, a link to the privacy

parent may refuse to permit further contact with the child and require the deletion of the parent's and child's online contact information, and how the parent can do so; (v) That if the parent fails to	policy must be posted at the point of purchase. • For all products supplied directly to schools, a copy of

respond to this direct notice, the operator may use the online contact information collected from the child for the purpose stated in the direct notice; and (vi) A hyperlink to the operator's online notice of its information practices required under § 312.4(d). (4) *Content of the direct notice to the parent required under § 312.5(c)(5) (Notice to a Parent In Order to Protect a Child's Safety).* This direct notice shall set forth: (i) That the operator has collected the name and the online contact information of the child and the parent in order to protect the safety of a child; (ii) That the information will not be used or disclosed for any purpose unrelated to the child's safety; (iii) That the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so; (iv) That if the parent fails to respond to this direct notice, the operator may use the information for the purpose stated in the direct notice; and (v) A hyperlink to the operator's online notice of its information practices required under § 312.4(d). (d) *Notice on the website or online service.* In addition to the direct notice to the parent, an operator must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its website or online service, *and,* at each area of the website or online service where personal information is collected from children. The link must be in close proximity to the requests for information in each such area. An operator of a general audience website or online service that has a separate children's area must post a link to a notice of its information practices with regard to children on the home or landing page or screen of the children's area. To be complete, the online notice of the website or online service's information practices must state the following: (1) The name, address, telephone number, and e-mail address of all operators collecting or maintaining personal information from children through the website or online	the privacy policy must be available to the school prior to completion of the sale, download or installation of the product. <u>Content of the Notice for Parental Consent</u> Member Companies must provide notice and obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children. The notice must be clearly and understandably written, complete, and must not contain any unrelated, confusing, or contradictory materials. The notice may contain an optional, brief statement explaining what the website or online service is. However, it may not contain marketing, sell or other promotional language. In all cases, it must be clear that a parent may agree to allow for the collection and use of a child's personal information without agreeing to the disclosure of that information to third parties, unless both are required in order to deliver a particular website or online service feature. There are different requirements for the content of the notice requesting parental consent, depending on the use case: • Request for Consent to Collect, Use or Disclose a Child's Personal Information: o This notification must include the following: ▪ That the operator has collected the parent's online contact information from the child, and, if applicable, the name of the child or the parent, in order to obtain the parent's consent; ▪ That the parent's consent is required for the collection, use, or disclosure of the information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide consent; ▪ Any additional items of personal information the

service. *Provided that*: the operators of a website or online service may list the name, address, phone number, and e-mail address of one	operator intends to collect from the child, and/or potential opportunities for the disclosure of personal

operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the website or online service are also listed in the notice; (2) A description of what information the operator collects from children, including whether the website or online service enables a child to make personal information publicly available; how the operator uses such information; and, the operator's disclosure practices for such information; and (3) That the parent can review or have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.	information, should the parent provide consent; ▪ How the parent can provide consent to the collection, use, and disclosure of the information; and ▪ That if the parent does not provide consent within a reasonable time from the date the notice was sent, the operator will delete the parent's online contact information from its records. ▪ A hyperlink to the Privacy Policy • Voluntary Notice of a Child's Online Activities Not Involving Collection, Use or Disclosure of Personal Information o This notice is optional, but when provided it must include the following: ▪ That the operator has collected the parent's online contact information from the child to provide notice to, and update the parent about, a child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information; ▪ That the parent's online contact information will not be used or disclosed for any other purpose; ▪ That the parent may refuse to permit the child's participation in the website or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and ▪ A hyperlink to the Privacy Policy • Notice of Intent for Multiple Contact o This notice must include the following: ▪ That the operator has collected the child's online contact information from the child to communicate with the child more than once; ▪ That the operator has collected the parent's online

	contact information child to notify the parent that the child has registered to receive multiple online communications from the operator; ▪ That the online contact information collected from the

	child will not be used for any other purpose, and that it will not be disclosed, or combined with any other information collected from the child; ▪ That the parent may refuse to permit further contact with the child and require the deletion of the parent's and child's online contact information, and how the parent can do so; ▪ That if the parent fails to respond to the notice, the operator may use the online contact information collected from the child for the stated purpose; and ▪ A hyperlink to the Privacy Policy • Notice to Protect Safety o This notice must include the following: ▪ That the operator has collected the name and the online contact information of the child and the parent in order to protect the safety of a child; ▪ That the information will not be used or disclosed for any other purpose; ▪ That the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so; ▪ That if the parent fails to respond to the notice, the operator may use the information for the stated purpose; and ▪ A hyperlink to the Privacy Policy

§ 312.5 Parental consent. *(a) General requirements.* (1) An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children, including consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented. (2) An operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.	Parental Control of Children's Data Parents should remain in control of data collected from their child. Providing parents with notice, choice and consent over whether or not their child's data is collected, and whether or not it is used or disclosed, should be maintained at all times while an operator intends to collect data from a child or is in possession of a child's data. This includes providing parents with a reasonable means to review the specific data or categories of data that may have been collected from their child, allowing them to request that it be deleted, and/or that the operator not collect any further data from the child.

(b) Methods for verifiable parental consent. (1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. (2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include: (i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan; (ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder; (iii) Having a parent call a toll-free telephone number staffed by trained personnel; (iv) Having a parent connect to trained personnel via video-conference; (v) Verifying a parent's identity by checking a form of government issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; or (vi) *Provided that*, an operator that does not "disclose" (as defined by §312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email. (3) *Safe harbor approval of parental consent methods*. A safe harbor program approved by the Commission under § 312.11 may	Member Companies should have a process in place that takes into account available technology to provide for verification that the person requesting to review the data is the parent. <u>Prior Consent for Data Collection</u> Operators must obtain verifiable parental consent before collecting, using and/or disclosing personal information from children and must provide parents with notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented. In addition, Member Companies must give the parent the option to consent to the collection and use of the child's personal information without agreeing to disclosure of the child's personal information to third parties. Consent from Schools Member Companies contracting directly with a school 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. • Providing such consent in lieu of the parent is at the sole discretion of the school. • If the Member Company intends to use or disclose students' personal information for other commercial purposes, it must obtain prior consent directly from the parents <u>Methods for Obtaining Parental Consent</u> Member Companies must use one of the methods described below to verify that the person providing consent is the parent: • Provide parents with a consent form to be signed and returned via postal mail, facsimile or electronic scan • Require that the parent provide a credit card,

approve its member operators' use of a parental consent method not currently enumerated in paragraph (b)(2) where the safe harbor program determines that such parental consent method meets the requirements of paragraph (b)(1).	debit card or other online payment system that provides

(c) *Exceptions to prior parental consent.* Verifiable parental consent is required prior to any collection, use, or disclosure of personal information from a child *except* as set forth in this paragraph: (1) Where the sole purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent under § 312.4(c)(1). If the operator has not obtained parental consent after a reasonable time from the date of the information collection, the operator must delete such information from its records; (2) Where the purpose of collecting a parent's online contact information is to provide voluntary notice to, and subsequently update the parent about, the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(2); (3) Where the sole purpose of collecting online contact information from a child is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request; (4) Where the purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in § 312.4(c)(3). An operator will not be deemed to have made	notification of each discrete transaction, and use it in connection with a monetary transaction • Provide a toll-free number or video conference system staffed by personnel who have been trained to identify whether or not the caller is a parent • Check a parent's form of government-issued ID against databases of such information. (The ID must be deleted from the Member Company's records promptly after such verification is complete.) • Knowledge-based authentication, as long as the specific process uses dynamic, multiple-choice questions with enough options to ensure that the chances of a child guessing the correct answers is low and the questions used are of sufficient difficulty that it would be difficult for a child in the household to figure out the answers • Where a child's personal information is collected but not disclosed, an operator may send an email to the parent provided that the email is followed up after receipt of consent with one of the following: o A confirmation email to the parent o A letter or telephone call confirming the parent's consent, if such information has been received from the parent ▪ Either such follow-up must advise parents that they may revoke their prior consent if they choose to Alternate Methods for Obtaining Parental Consent Member Companies may propose additional methods for obtaining verifiable parental consent. Such proposals must include full details of the process envisioned, including what data will be captured, how it will be handled and who at the Member Company will be responsible for executing the process. Any such proposed method must be reasonably

reasonable efforts to ensure that a parent receives notice where the notice to the parent was unable to be delivered; (5) Where the purpose of collecting a child's and a parent's name and online contact information, is to protect the safety of a child,	calculated, in light of available technology, to ensure that the

and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with notice as described in § 312.4(c)(4); (6) Where the purpose of collecting a child's name and online contact information is to: (i) protect the security or integrity of its website or online service; (ii) take precautions against liability; (iii) respond to judicial process; or (iv) to the extent permitted under other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety; and where such information is not be used for any other purpose; (7) Where an operator collects a persistent identifier and no other personal information and such identifier is used for the sole purpose of providing support for the internal operations of the website or online service. In such case, there also shall be no obligation to provide notice under § 312.4; or (8) Where an operator covered under paragraph (b) of the definition of *website or online service directed to children* collects a persistent identifier and no other personal information from a user who affirmatively interacts with the operator and whose previous registration with that operator indicates that such user is not a child. In such case, there also shall be no obligation to provide notice under § 312.4.	person providing consent is the child's parent. Proposals will be evaluated by the iKeepSafe Safe Harbor program to determine whether or not the methods meet these stated requirements and will be considered acceptable under the iKeepSafe Safe Harbor program. Any such determination and approval will be at iKeepSafe Safe Harbor program's sole discretion. Exceptions to Obtaining Prior Parental Consent: In certain use cases as described below, prior parental consent is not required: • When the only purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent o The information must be deleted from the operator's records if parental consent is not received after a reasonable time • When the purpose of collecting a parent's online contact information is to provide voluntary notice to, and update the parent about, the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information. o In these cases, the parent's online contact information may not be used for any other purpose o Reasonable efforts, taking into account available technology, must be taken to ensure that the person receiving the notice is the parent • When the only purpose of collecting online contact information from a child is to respond once to a specific request from a child. The information may not be disclosed or used for any other purpose, including to contact the child more

	than once ○ The information must be deleted from the

	Member Company's records promptly after responding to the child's request • When the purpose of collecting a child's and a parent's online contact information is to respond directly, more than once, to a child's specific request, such as a request to sign up for an operator's newsletter. o The information may not be used for any other purpose, and may not be disclosed or combined with any other information collected from the child o Although prior consent is not required for the first contact, Member Companies must provide parents with notice of the information that was collected, what it is being used for, that parents may opt their child out of further contact and how to do so, all prior to the second contact with the child. For requirements, see Content of the Notice for Parental Consent Section below. • When the purpose of collecting a child's name and online contact information is to: o Protect the security and/or integrity of its website or online service o Take precautions against liability o Respond to a judicial process o Provide information to law enforcement agencies or for an investigation on a matter related to public safety to the extent permitted by law and where such information is not being used for any other purpose • When a persistent identifier is collected *for the sole purpose of providing support for internal operations* (as defined above) for their website or online service.

§ 312.6 Right of parent to review personal information provided by a child. (a) Upon request of a parent whose child has provided personal	Privacy Policy: Description of what personal and non-personal information the operator collects from users, including:

information to a website or online service, the operator of that website or online service is required to provide to that parent the following: (1) A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, e-mail address, hobbies, and extracurricular activities; (2) The opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information; and (3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the operator to carry out this provision must: (i) Ensure that the requestor is a parent of that child, taking into account available technology; and (ii) Not be unduly burdensome to the parent. (b) Neither an operator nor the operator's agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section. (c) Subject to the limitations set forth in § 312.7, an operator may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the operator's further use or collection of personal information from his or her child or has directed the operator to delete the child's personal information.	• that a parent has the right to review, have deleted and/or refuse to permit further collection or use of the child's information, along with information on how to do so <u>Parental Control of Children's Data</u> Parents should remain in control of data collected from their child. Providing parents with notice, choice and consent over whether or not their child's data is collected, and whether or not it is used or disclosed, should be maintained at all times while an operator intends to collect data from a child or is in possession of a child's data. This includes providing parents with a reasonable means to review the specific data or categories of data that may have been collected from their child, allowing them to request that it be deleted, and/or that the operator not collect any further data from the child. Member Companies should have a process in place that takes into account available technology to provide for verification that the person requesting to review the data is the parent.

§ 312.7 Prohibition against conditioning a child's participation on collection of personal information. An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.	Minimization of Data Collection In the arena of product development, media and marketing intended for children, collection of data should be limited to only what is reasonably required to deliver a promised product, feature or service to a child user and to such data reasonably needed to maintain and further develop the website or service. Limitations on Collection of Data Member Companies may only collect 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.

	Collection of more data than is reasonably necessary to provide features, activities or support for internal operations is not acceptable. Collection of all personal information must comply with the parental notice and consent requirements outlined above, and all such data collection and handling practices must be disclosed in the privacy policy.
§ 312.8 Confidentiality, security, and integrity of personal information collected from children. The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The operator must also take 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.	Security Operators must take responsibility for safeguarding data collected from or about their users. Reasonable measures must be taken to secure and maintain the confidentiality, security and integrity of data. Such measures must also include practices for regularly deleting data within a reasonable time frame after it is no longer being used or is no longer needed. Data Security, Confidentiality and Integrity Data must be stored securely, with sensitive data, such as personal information, stored separately from other data. • Access to data must be limited to authorized employees, and a procedure must be in place to revoke access when an employee leaves the organization. • Inactive data must be purged on a regular basis, with a defined process in place for deleting and destroying said data. • A defined process must also be in place for deleting and destroying data when requested by a parent o This process must include steps to confirm that the person requesting review or deletion of a child's data is the parent • A defined process must exist for conducting regular security audits. Third Party Service Providers

	Member Companies must establish procedures and practices for: • informing any third party service providers that its site

	or online service is directed to children • informing any third party service providers of its data privacy and security policies and practices • receiving written assurances that any third party service providers are able to comply with those policies and practices Third Party Assessment Requirements Member Companies must assess the privacy policies and practices of any third party service providers to ensure that they are capable of complying with Member Company's policies and practices, including those related to the collection, use, transfer, confidentiality, security and integrity of user data. • Member Companies must receive affirmative assurances from third parties to that effect • Such procedures, assessments and assurances related to third party service providers must be repeated on an annual basis, at any time at which Member Company's policies or practices change, and at any time that they are made aware of changes in a third party provider's policies or practices. Any such changes must also be reported to iKeepSafe Safe Harbor program for assessment. • Certification that these requirements have been met must be submitted to iKeepSafe Safe Harbor program as part of the initial certification and annual renewal process.

§ 312.10 Data retention and deletion requirements. An operator of a website or online service shall retain 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. The operator must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.	Security Operators must take responsibility for safeguarding data collected from or about their users. Reasonable measures must be taken to secure and maintain the confidentiality, security and integrity of data. Such measures must also include practices for regularly deleting data within a reasonable time frame after it is no longer being used or is no longer needed. Data Security, Confidentiality and Integrity Data must be stored securely, with sensitive data, such as

personal information, stored separately from other data.

- Access to data must be limited to authorized employees, and a procedure must be in place to revoke access when an employee leaves the organization.
- Inactive data must be purged on a regular basis, with a defined process in place for deleting and destroying said data.
- A defined process must also be in place for deleting and destroying data when requested by a parent
    - This process must include steps to confirm that the person requesting review or deletion of a child's data is the parent
- A defined process must exist for conducting regular security audits.

<u>Third Party Service Providers</u>

Member Companies must establish procedures and practices for:

- informing any third party service providers that its site or online service is directed to children
- informing any third party service providers of its data privacy and security policies and practices
- receiving written assurances that any third party service providers are able to comply with those policies and practices

Third Party Assessment Requirements

Member Companies must assess the privacy policies and practices of any third party service providers to ensure that they are capable of complying with Member Company's policies and practices, including those related to the collection, use, transfer, confidentiality, security and integrity of user data.

- Member Companies must receive affirmative assurances from third parties to that effect

- Such procedures, assessments and assurances related

	to third party service providers must be repeated on an annual basis, at any time at which Member Company's policies or practices change, and at any time that they are made aware of changes in a third party provider's policies or practices. Any such changes must also be reported to iKeepSafe Safe Harbor program for assessment. ● Certification that these requirements have been met must be submitted to iKeepSafe Safe Harbor program as part of the initial certification and annual renewal process.