Revised Exhibit C of kidSAFE's COPPA Safe Harbor Application

Full Text of FTC-Approved kidSAFE+ Certification Guidelines

---

kidSAFE® Seal Program
Certification Rules – version 3.0 (FINAL)

Effective as of February 1, 2014

The kidSAFE Seal Program (KSP) is a fast-growing safety certification service and seal of approval program designed exclusively for children-friendly websites and applications, including kid-targeted game sites, educational sites, virtual worlds, social networks, mobile apps, tablet devices, and other similar interactive services and technologies (collectively, "sites or services").

The Program currently offers two certification seals – kidSAFE and kidSAFE+. To qualify for the basic kidSAFE Seal, the site or service being reviewed must be found compliant with our Basic Safety Rules, which are reflected under Sections 1-5 below. To qualify for the kidSAFE+ Seal, the site or service must be found compliant with our Basic Safety Rules, as well as our Additional Privacy Rules which are reflected under Sections 6-11 below. The Additional Privacy Rules are modeled after the revised Children's Online Privacy Protection Rule ("Revised COPPA Rule" or "COPPA"), which went into effect on July 1, 2013. Only those sites and services that first become paying members in our program are eligible to be reviewed for kidSAFE+/COPPA certification.

Please note that any rules listed as "optional" are only recommended (not required) to achieve certification for that level. However, for basic kidSAFE certification, optional rules may be treated as mitigating factors in the absence of full compliance with certain other mandatory rules. Any rules preceded by other limitations (e.g., "mobile apps only", "devices only", etc.) suggest that those rules apply only to that particular technology or service. Please also consult the footnotes at the end of this document, and (when prompted) the relevant text of the Revised COPPA Rule[1] (attached as an Addendum hereto), as both are essential to the appropriate interpretation and application of these Certification Rules.

These KSP Certification Rules are subject to change at any time, with notice to our members. If any material changes are made to the Additional Privacy Rules (i.e., Sections 6-11), such changes will be submitted to the Federal Trade Commission (FTC) for prior approval in accordance with the COPPA Safe Harbor requirements. Unless required otherwise by the FTC for changes to Sections 6-11, all changes to these Rules will be applied on a go-forward basis only.

[1]Sections 6-11 of these Certification Rules are designed to be fully consistent with, all-encompassing of, and, in some areas, even stricter than the Revised COPPA Rule which went into effect on July 1, 2013. If, however, there appear to be any provisions in the Revised COPPA Rule (including any definitions of terms) that are not explicitly covered under Sections 6-11 of these Rules, then the relevant provisions of the Revised COPPA Rule shall be incorporated into Sections 6-11 of these Rules and binding upon our kidSAFE+/COPPA seal members.

Basic Safety Rules

1. Chat and other interactive community features must be designed with safety protections and controls

[detailed sub-rules redacted for proprietary reasons, as they are not specific to COPPA]

2. Must post rules and educational information about online safety

[detailed sub-rules redacted for proprietary reasons, as they are not specific to COPPA]

3. Must have procedures for handling safety issues and complaints

[detailed sub-rules redacted for proprietary reasons, as they are not specific to COPPA]

4. Must give parents basic safety controls over their child's activities

[detailed sub-rules redacted for proprietary reasons, as they are not specific to COPPA]

5. Content, advertising, and marketing must be age-appropriate

[detailed sub-rules redacted for proprietary reasons, as they are not specific to COPPA]

Additional Privacy Rules (kidSAFE+/COPPA certification only)

6. Age screening mechanisms (when used) must be neutral

(a) *Age screening mechanisms must only be used when appropriate under COPPA*[41]

(b) *Age screening mechanisms must not force or entice kids to enter false age information (e.g., the fields should offer a full selection of target ages, no "check here" boxes*[42]*, etc.)*

(c) *The wording displayed around age screening mechanisms (or at any point during the registration process) must not entice kids to provide false age information*[43]

(d) *Must not completely lock out kids under 13 from using your site/service*[44]

Optional rules

(e) *[optional] – Should use technological measures (e.g., session cookies) to help prevent age falsification (i.e., kids clicking back and changing their original age selection)*

7. Must notify and obtain prior verifiable consent from a parent[45] when required by the COPPA Rule

(a) *Must notify and obtain consent from a parent before collecting and storing a child's personal information*[46] *in connection with registration or account creation*[47]

(b) *Must notify and obtain consent from a parent before giving a child access to features that allow the sharing of personal information in a public setting or with other users (e.g., chat, in-game messaging, community features, profile pages, blogs, status updates, public contents and promotions, etc.)*[48]

(c) *Must notify and obtain consent from a parent before giving a child access to send-to-friend features that allow the sharing of personal information*[49]

(d) *Must notify and obtain consent from a parent before giving a child access to third party plug-in features (such as third party share functionalities, login features, etc.*[50]*) that collect personal information through your site or service*[51]

(e) *Must notify and obtain consent from a parent before collecting and uploading a child's geolocation information (some exceptions apply*[52]*)*

(f) *Must notify and obtain consent from a parent before collecting or using a child's personal information in connection with sending the child ongoing newsletters or other alerts (e.g., push notifications)*[53]

(g) *[catch-all requirement] – Must notify and obtain consent from a parent before collecting a child's personal information in connection with any other features or activities (e.g., customer support forms, non-public contests and promotions, uploading of user-generated-content, etc.)*[54]

(h) *Must notify and obtain consent from a parent before collecting and using a persistent identifier*[55]*, unless such persistent identifier is used for internal support purposes only*[56]

(i) *Must notify and obtain consent from a parent before sharing a child's personal information with independent third parties*[56A]

(j) *Must give parents the option to consent to the collection and use of their child's personal information (as set forth under Rules 7(a)-(h) above) without having to consent to the disclosure of their child's personal information to independent third parties*[56B]

(k) *Must notify and obtain consent from a parent before collecting or using a child's personal information for significantly new purposes not previously consented to by the parent (e.g., giving a child access to new data sharing features)*

(l) *Any parental notices required under this Section must meet COPPA's "direct notice" requirements*[57]

(m) *Any parental consent mechanisms required under this Section must meet COPPA's "verifiable parental consent" requirements*[58]

(n) *Must not collect more personal information from children than is allowed under COPPA prior to obtaining parental consent*[59]

(o) *When parental consent is required, must delete a child's personal information if the parent's consent is not received within a reasonable amount of time (e.g., 7-14 days)*

8. Must give parents access to their child's personal information[60]

(a) *Must allow parents to review*[61] *their child's personal information*

(b) *Must allow parents to stop further collection or use*[62] *of their child's personal information*

(c) *Must allow parents to delete*[63] *their child's personal information*

(d) *Must not allow parents to access or make changes to their child's personal information without prior authentication*[64]

(e) *Must provide mechanism for parents to inquire or submit complaints about privacy related issues*[65] *(e.g., data usage questions, account hijackings, unsubscribe requests, etc.)*

9. Must protect the integrity and security of a child's information

(a) *Must minimize the amount of personal information collected/stored from a child to that which is reasonably necessary for each activity*[66]

(b) *The registration process for a child's account must be reasonably secure (e.g., no GET method, no use of real name as username, masking of passwords, minimum password length/strength, etc.)*

(c) *The account access and retrieval process for a child's account must be reasonably secure (e.g., username and password required for login, secure "forgot password" and "forgot username" mechanisms, secure "remember-me" feature, etc.)*

(d) *Must have stronger protections for collection/transmission of sensitive account information (e.g., encryption for credit card transactions)*

(e) *Must have reasonable electronic safeguards to protect a child's personal information while it is stored (e.g., firewall-protected servers, intrusion detection testing, internal access controls, etc.)* [67]

(f) *Must have reasonable manual safeguards to protect a child's personal information while it is stored (e.g., confidentiality agreements with employees, secure locations for servers and paper records, etc.)* [68]

(g) *Must take reasonable steps*[69] *to check that any service providers and third parties with whom children's personal information is shared are capable of protecting the information shared with them*

(h) *Must obtain written assurances*[70] *from services providers and third parties that they will protect any children's personal information shared with them*

(i) *Must take reasonable steps to check that any service providers or third parties that collect information on your behalf for internal support purposes (such as for analytics or contextual advertising) do not also merge such data with behavioral advertising data*[71]

(j) *Must delete children's personal information after it is no longer needed*[72]

(k) *Any deletion of children's personal information must be done securely*[73]

10. Must post a COPPA-compliant privacy policy[74]

(a) *Must post a children's privacy policy*[75] *if your site/service collects any personal information from kids*

(b) *Links to the policy must be displayed prominently as required by COPPA*[76]

(c) *Links to the policy must be displayed in the locations required by COPPA*[77]

(d) *The policy must contain all applicable COPPA-required disclosures*[78]

(e) *The policy must be truthful, comprehensive, easy-to-understand, and free of irrelevant or confusing information*[79]

(f) *The policy must be updated to reflect important changes in the site/service's data handling practices*

(g) *Upon a general request from a parent, must inform the parent of the specific types of personal information collected from kids*

11. Must cooperate with the kidSAFE Seal Program (KSP)'s oversight and enforcement mechanisms

(a) *Must cooperate with KSP's compliance reviews, including initial and annual compliance assessments, random seeding and testing of interactive features (such as sign-up forms, chat features, etc.), and periodic monitoring of data usage practices (e.g., review of marketing communications)*

(b) *Must address all safety and privacy-related consumer complaints forwarded by KSP in a timely and satisfactory manner*

(c) *When material violations occur*[80]*, must cooperate with KSP's enforcement mechanisms, which may include increases in membership fees, termination of membership (including removal of all seals), consumer redress, and/or anonymous payments to the United States Treasury*[81]

(d) *Must submit to KSP any material changes in your product features or practices (such as changes to registration flows, parental consent techniques[82], chat features, data collecting features, data usage practices, privacy policy statements, etc.) for prior review and approval*

FOOTNOTES FOR SECTION 6

[41] Age screening mechanisms are questions that ask for a user's age or date of birth to verify whether the user is old enough to access or participate in a particular activity. These mechanisms should only be used in certain circumstances, depending on the targeted age demographic of the site or service. For example, if you operate a site, mobile app, or other service that is exclusively intended for children under the age of 13 (see next paragraph for determining factors), you must assume that all of your users are under that age and follow COPPA requirements, regardless of the actual age of every user. By contrast, if you operate a site or service that is directed to children as well as older users (teens, parents, etc.), and so children are not the "primary target", then you would have the option to use an age screen mechanism and either prevent collection of personal information from children under 13 or allow collection from them in accordance with COPPA requirements. *See paragraph (c) of the definition of "Website or online service directed to children" under Section 312.2 of Revised COPPA Rule.* An age screen mechanism may also be appropriate if you operate a general-audience site or service that appeals to users of all ages, in which case the COPPA requirements would be triggered if you have actual knowledge that you're collecting personal information from a child (whether through your own site/service or the site/service of someone else). *See paragraph (b) of the definition of "Website or online service directed to children" under COPPA.* In all cases, under COPPA, you may NOT entirely block children under 13 from using your site or service, as noted under Rule 6(d) of these Certification Rules. Note that registration forms on child-directed sites and services may never be directed to parents solely for the purpose of avoiding COPPA requirements. Despite everything stated in this footnote, there are some scenarios when age or date of birth information may be collected for non-age-screening purposes (such as to collect user demographics as part of an anonymous registration feature or in connection with some other COPPA-compliant registration feature). Every age-screening scenario will be carefully assessed by KSP on a case-by-case basis to help ensure compliance with COPPA and the spirit of COPPA.

To determine whether your site or service is "directed toward children", you should consider all of the following factors about your site or service:

- subject matter
- visual content
- use of animated characters or child-oriented activities and incentives
- music and other audio content
- age of models
- presence of child celebrities or celebrities who appeal to children
- language or other characteristics of your site or service
- whether ads promoting your site or service appear on other child-directed sites/services
- whether ads appearing on your site or service are directed to kids
- evidence regarding the actual, intended, or likely audience of your site or service
- (whether offline merchandise associated with your site or service is marketed to kids)
- (which platforms/devices is your site or service offered on and how is it categorized by third parties, such as the Apple App Store).

See paragraph (a) of the definition of "Website or online service directed to children" under Section 312.2 of Revised COPPA Rule.

[42] These are check boxes that simply ask users to click a button to confirm they're at least 13 years of age (or some other minimum age) instead of prompting them to enter age information.

[43] For example, the age screening mechanism must NOT display a message that tells users how old they need to be to register as a non-child user (for example, "Sorry, you need to be at least 13 years old to register"). This type of messaging may entice kids to lie about their age to avoid parental oversight.

[44] To qualify for certification under the kidSAFE Seal Program and warrant display of our seal, the site or service being reviewed must allow for children's participation or access at some level. If the service entirely blocks out children (either technologically or via its terms-of-use agreement), then our seal(s) may not be relevant to that particular service. In certain circumstances, the Revised COPPA Rule also does not allow for the complete blocking of children users. *See FN 41 above.*

FOOTNOTES FOR SECTION 7

[45] For purposes of these Certification Rules, a "parent" includes a legal guardian and (in some cases) may include a school or teacher. *See FN 58 below for additional information*.

[46] For purposes of this rule and other applicable kidSAFE+/COPPA rules under Sections 6-11, the meaning of a "child" is someone under the age of 13 years old. The meaning of "personal information" is as defined under Section 312.2 of the Revised COPPA Rule. In that section, the following data elements are defined as "personal" when collected from a child:

- First and last name (together);
- Home address or other physical address that includes street name and name of city or town;
- Online contact information (email address, IM identifier, VoIP identifier, video chat ID, other ID that permits direct contact online);
- Screen name or user name when it functions in the same manner as "online contact information" (*see bullet directly above*);

- Telephone number (landline, cell, etc.);
- Social security number;
- Persistent identifier that can be used to recognize a user over time and across different sites or services (e.g., IP address, unique device ID, processor or device serial number, customer number held in a cookie, etc.);
- Photo, video, or audio file when such file contains the image or voice of a child;
- Geolocation information sufficient to identify street name and name of city or town;
- Other information regarding a child or parent that is combined with any of the items listed above.

[47] There are some exceptions to this rule. For example, if no personal information is collected as part of registration (instead, only anonymous login information such as screen name and password is collected), then parental notice and consent may not be required. Similarly, COPPA allows for collection and use of a parent's email address or other online contact information (without prior parental consent) for purposes of: (a) obtaining parental consent (*see Section 312.5(c)(1) of Revised COPPA Rule*), (b) notifying and updating a parent about a child's account (*see Section 312.5(c)(2) of Revised COPPA Rule*), or (c) responding to certain safety, security, or legal issues (*see Section 312.5(c)(5)-(6) of Revised COPPA Rule*). These exceptions, however, only allow for a limited amount of data collection and have other usage or retention restrictions (e.g., non-use for other purposes, purging of the data collected after use is complete or if consent is not obtained, etc.). *See Section 312.5(c) of Revised COPPA Rule for further guidance.* Also note that some of these exceptions may have special parental notice requirements which are described in detail under Section 312.4(c) of the Revised COPPA Rule. *Also see FN 57 below.*

[48] If a company takes "reasonable measures" (e.g., automated filtering, human moderation, etc.) to delete all or virtually all instances of personal information from a child's postings before they can be made public (or shared with other users), and also takes steps to delete such information from its back-end records, then parental notice and consent would not be required for these types of features. *See Section 1 of these Certification Rules for further guidance on what might be considered "reasonable measures". Also see definitions of the terms "collects or collection" and "delete" under Section 312.2 of the Revised COPPA Rule.*

[49] Send-to-friend, e-cards, other similar features can be constructed in such a way that avoids the requirement for parental notice and consent. For example, if the feature is designed to only collect the "first name" of the sender and the email address(es) of friend(s) to whom the message will be sent (but does NOT also request the email of the sender or allow for a customized message to be entered), and then, immediately after the message is sent, the friends' email addresses are purged, then the feature would conform with COPPA's one-time-use exception (*specifically, Section 312.5(c)(3)*) and therefore not require prior parental notice or consent). Measures must be taken, however, to prevent the child who is sending the message from being able to enter more than just his/her "first name" on the send-to-friend form (for example, through character or space limitations).

[50] Examples of third party plug-in features that may be covered under this rule include:

- third party login features (such as Facebook Connect, Yahoo, Google, etc.);
- third party share features/widgets (such as Facebook Share, Twitter, Pinterest, Instagram, AddThis, etc.);
- third party like features (such as Facebook Like, etc.) – *see Section 312.5(c)(8) of Revised COPPA Rule for possible exception*;
- social gaming plug-ins (such as Apple Game Center, console-gaming networks, etc.); and,
- downloadable third-party toolbars.

Third party ad plug-ins that involve behavioral tracking are not listed above, as KSP's Basic Safety Rules do not presently allow for behavioral advertising. Note, however, that plug-ins used only for contextual advertising purposes are allowed under our program and would be exempt from COPPA's parental notice and consent requirement if implemented in accordance with Section 312.5(c)(7) of the Revised COPPA Rule.

The features listed may be covered under COPPA regardless of whether they send data back to your site or service. This is because you are seen as benefiting in other ways (e.g., marketing value, convenience, etc.) by their integration on your site or service. *See definition of the term "collected or maintained on behalf of" under Section 312.2 of Revised COPPA Rule.* PLEASE NOTE THIS IS AN AREA OF THE LAW WHERE YOU CAN BE HELD STRICTLY LIABLE IF NOT FULLY COPPA COMPLIANT. WE STRONGLY URGE YOU TO CONSULT WITH YOUR KSP REPRESENTATIVE FOR FURTHER GUIDANCE ON THIS TOPIC.

[51] If, however, your child-directed site or service merely provides a link off to a third party site or service (such as a button link to a Facebook fan page, Twitter page, etc.) but does not actually embed a data-collecting plug-in feature into your site/service, then parental notice and consent would not be required for such links. Note that in some instances an embedded plug-in feature may be allowed even without prior parental notice/consent, such as if it is placed in an entirely separate section of your site/service legitimately designated for parents or users 13 and older or if it conforms with the exception under Section 312.5(c)(8) of the Revised COPPA Rule. However, merely asking for age information prior to enabling such features may not always be sufficient. AGAIN, PLEASE NOTE THIS IS AN AREA OF THE LAW WHERE YOU CAN BE HELD STRICTLY LIABLE IF NOT FULLY COPPA COMPLIANT. WE STRONGLY URGE YOU TO CONSULT WITH YOUR KSP REPRESENTATIVE FOR FURTHER GUIDANCE ON THIS TOPIC.

[52] For parental notice and consent to be required, the geolocation information being collected must be detailed enough to identify street name and name of city or town. *See paragraph (i) of the definition of "personal information" under Section 312.2 of Revised COPPA Rule.* A precise location on a map or longitude/latitude coordinates is sufficiently detailed enough. However, a 5-digit zip code or other general coarse location would likely not be considered detailed enough, and therefore would not require prior parental notice and consent. Parental notice and consent

would also not be required if the geolocation information collected, even if detailed, is never uploaded back to the operator or developer (i.e., it is kept locally on the device only and never transmitted back to the operator online). *See FTC COPPA FAQ A4 for the proper handling of geolocation information collected/uploaded prior to July 1, 2013.*

[53] There is an exception to this rule. COPPA allows for the collection and use of a child's email address or other online contact information (without parental consent) for the purpose of sending the child multiple communications for a specific purpose (for example, e-mail newsletters, multiple contest announcements, mobile push notifications, etc.). This exception, however, only allows for the collection of "online contact information" (see definition under FN 46 above) and has other usage and data retention restrictions (e.g., non-use for other purposes, no combining the data with other personal information, etc.). In addition, to fulfill this exception, the parent must first be notified about this activity (via email, for example) and given the opportunity to opt-out their child from future communications. *See Sections 312.5(c)(4) and 312.4(c)(3) of Revised COPPA Rule for further guidance or consult with your KSP representative.*

[54] There is an exception to this rule. COPPA allows for the collection and use of a child's email address or other online contact information (without parental notice or consent) for features or activities that involve a one-time use (e.g., contest entry, customer support inquiry, one-time email announcement, etc.). This exception, however, only allows for the collection of "online contact information" (see definition under FN 46 above) and has other usage and data retention restrictions (e.g., non-use for other purposes, purging of the data after the one-time use is complete, etc.). *See Section 312.5(c)(3) of Revised COPPA Rule for further guidance or consult with your KSP representative.*

[55] Examples of persistent identifiers may include an IP address, unique device ID, processor or device serial number, customer number held in a cookie, or other similar identifier. *Also see FN 46 above regarding definition of "personal information".*

[56] When a persistent identifier (such as those listed under FN 55 above) is used solely to support the internal operations of a child-directed website or service and is not combined with other personal information (*see FN 46 above*), then it is exempt from this parental notice and consent requirement. This is known as the "support for internal operations" exception under COPPA. Currently, the following data usage activities are considered "support for internal operations" as such term is defined under Section 312.2 of the Revised COPPA Rule:

- maintaining or analyzing the functioning of the site or service (e.g., analytics);
- performing network communications;
- authenticating users;
- personalizing content on the site or service (but not for purposes of showing behaviorally-targeted ads);
- serving contextual ads;
- capping the frequency of ads;
- protecting the security or integrity of the user, website, or online service;
- ensuring legal or regulatory compliance; or,
- fulfilling a request from a child under the one-time-contact or multiple-contact exceptions of COPPA (*see FNs 53 and 54 above*).

To qualify for the exception, the persistent identifier collected and used for the activities above must not also be used to contact a specific individual (including through behavioral advertising), to amass a profile on a specific individual, or for any other purpose. The FTC has the authority to add new activities to the list above, following a special review and approval process defined under Section 312.12(b) of the Revised COPPA Rule.

[56A] Note, however, that the sharing of children's personal information with third party service providers who merely provide support for the internal operations of your site or service (and who do not use the data for any other purpose) would not be considered "sharing with *independent* third parties" for purposes of this rule. The same would be true for two separate companies that simultaneous collect children's personal information on a jointly-operated or jointly-sponsored website or service. Such co-operators of a site or service would not be considered "*independent* third parties" for purposes of this rule. However, each of these co-operators would have its own, separate obligation to comply with COPPA. *For further guidance, see definitions of the terms "disclose or disclosure", "release of personal information", and "third party" under Section 312.2 of the Revised COPPA Rule.*

Also, when considering this Rule 7(i), it is important to note that Rule 5(g) of these Certifications Rules currently prohibits the selling or sharing of children's personal information with independent third parties for marketing purposes. Therefore, this Rule 7(i) would only be relevant in cases where a child's personal information is being shared with independent third parties for non-marketing purposes (such as for research studies).

[56B] *See FN 56A above. Also see Section 312.5(a)(2) of Revised COPPA Rule and FTC COPPA FAQ H9.*

[57] These direct notice requirements are highly unique and detailed to each direct notice scenario. *See Section 312.4(c) of Revised COPPA Rule for further guidance on these requirements or consult with your KSP representative.* In all cases, however, the site or service must take reasonable steps to ensure that the parent of the child has in fact received the direct notice (*see Section 312.4(b) of Revised COPPA Rule*). For example, if the site or service receives a bounce-back email message indicating that the notice was undeliverable, then the direct notice would be deemed to have not been received.

[58] This entails using a method of parental consent that is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent (*see Section 312.5(b)(1) of Revised COPPA Rule)*. The FTC has enumerated several methods that already meet this standard (*see Section 312.5(b)(2) of Revised COPPA Rule)*. They are as follows:

- For internal uses of a child's information (i.e., when a child's personal information will be used for internal purposes only and will not be shared with other companies or users), "Email Plus" consent may be used. Email Plus consent involves obtaining parental consent via email communication (for example, by sending an activation link to the parent via email), followed by a delayed confirmatory step (such as sending a second email upon receipt of the parent's consent). The confirmatory notice must state that the parent can revoke his/her consent given in response to the earlier email and explain how the parent can do so.
- For disclosures of a child's information (i.e., when a child's personal information may be posted publicly or shared with other users or entities), a "more reliable" form of parental consent must be used. Email Plus would not be sufficient. Currently, the following methods of consent are considered "more reliable": (1) having the parent sign a printed consent form and send it back to you via fax, mail, or electronic scan, (2) having the parent use a credit card, debit card, or other online payment system (such as PayPal) in connection with a monetary transaction and that provides notification of each transaction to the primary account holder, (3) having the parent call a toll-free telephone number staffed by live/trained personnel, (4) having the parent connect to live/trained personnel via video conference, (5) having the parent provide a government-issued ID (e.g., driver's license, SSN, etc.) that you verify against a database of such information, so long as the ID information is deleted from your records promptly after the verification is complete, or (6) having a parent use another method pre-approved by the FTC or an FTC-approved COPPA safe harbor program pursuant to the Revised COPPA Rule. *See Sections 312.12(a) and 312.5(b)(3) of Revised COPPA Rule for further details about the process of submitting a new parental consent method for approval.*.

Please note that *merely* directing a child to have the parent register on the child's behalf or to go ask their parent for permission before signing up is never a sufficient means of obtaining parental consent. In some instances (such as for online activities in the school context), you may be allowed to notify and obtain consent from a school teacher or the school itself in lieu of a parent or other legal guardian. *See FTC COPPA FAQs M1-M4 for further guidance on school-based consent, or consult with your KSP representative.*

[59] Prior to obtaining parental consent (and for the very purpose of obtaining consent), COPPA allows you to collect a very limited amount of personal information from a child, such as the child's name, parent's name, child's email address, parent's email address, or other online contact information (*see Section 312.5(c)(1) of the Revised COPPA Rule*). The Rule may also allow you to collect other non-personal information essential to the account creation and consenting process (e.g., password, screen name or user name that does not function as online contact information). However, a fuller profile of the child may not be created prior to providing notice and obtaining consent pursuant to COPPA.

FOOTNOTES FOR SECTION 8

[60] The parental access rights referenced in this Section 8, when applicable, need not be automated or web-based. For example, *manual* processing of a parent's request to review their child's personal information or have it deleted would be acceptable in lieu of an automated or web-based mechanism. Also, these rights (parental access, deletion, etc.) need only be honored upon specific request from a parent. A parent should also be able to make these access requests rather easily (i.e., without an overly burdensome process) and free of charge (i.e., without having to pay a fee or be a paying member of the site/service). *See Section 312.6(a) of Revised COPPA Rule.*

[61] This rule does not require that you store the child's personal information in order for the parent to have access to it later. In other words, if you decide to delete the child's personal information (for policy or other reasons), you can simply reply that you no longer have any personal information stored about the child. If, however, you choose to store the information for legitimate ongoing use and with the appropriate parental permission, then you must enable the parent to access the information for review at any time. *See Section 312.6(a)(3) of Revised COPPA Rule.*

[62] This may include, for example, allowing the parent to stop the sending of marketing communications to the child (if the site does this) or allowing the parent to stop additional collection or use of their child's personal information in connection with other features (such as a social profile page or photo/video contest). If a parent makes a request of this kind, the site or service may prevent the child from accessing the site or service (or certain features within the site or service) in the future. *See Section 312.6(c) of Revised COPPA Rule.*

[63] Any deletion of the child's personal information (done in response to a parent's request) must be done securely, in accordance with Rule 9(j) of these Rules. If a parent requests deletion of their child's personal information, the site or service may prevent the child from accessing the site or service (or certain features within the site or service) in the future. *See Section 312.6(c) of Revised COPPA Rule.*

[64] Prior authentication of a parent can be achieved in a variety of ways, but must attempt to ensure (taking into account available technology) that the person requesting access is in fact the child's parent. *See Section 312.6(a)(3) of Revised COPPA Rule.* For example, before granting access, the parent should be required to verify at least one of the following: (i) the child's unique login credentials (username, password, etc.), (ii) separate password/PIN information created for the parent or parent account, or (iii) other information that uniquely identifies the child or the child's account and that only the parent would know. If, after taking these reasonable measures, you nonetheless give out a child's personal information to someone who is not the child's parent or guardian, you or any agent acting on your behalf will not be held liable under COPPA (*see Section 312.6(b) of Revised COPPA Rule*).

[65][65] A simple online contact form, or contact information (such as a contact email address) displayed within a privacy policy, would suffice for purposes of this rule.

FOOTNOTES FOR SECTION 9

[66] In other words, if certain information is not needed for a child to participate in a specific activity or use a specific feature, then that information should not be collected or requested from the child (*see Section 312.7 of Revised COPPA Rule*). Merely labeling a field as "optional" would not suffice for purposes of meeting this rule (*see paragraph (a) of the definition of "collects or collection" under Section 312.2 of Revised COPPA Rule*).

[67] The actual safeguards required will depend on a variety of factors, including (among other things) the sensitivity of the personal information stored about children, the amount of personal information stored, the method of storage, and the size of the company operating the site or service.

[68] *See FN 67 above.*

[69] At a minimum, these steps should include a due diligence review of the third party's data security practices prior to the initial hiring or sharing of personal information with that third party, as well as periodic checks on the third party's data security practices thereafter.

[70] Preferably, these written assurances should be contractual, although other forms of written assurances may be acceptable in lieu of a contract (such as a statement or certificate asserting or demonstrating compliance with a widely-recognized data security standard (PCI, ISO, EU Safe Harbor, etc.).

[71] COPPA allows for the collection and use of IP addresses or other persistent identifiers (without parental notice and consent) for the purpose of gathering analytics about the use of your site or service, personalizing the content on your site/service, and showing contextual ads (*see FN 56 above for other allowable uses of persistent IDs*). However, that same data may NOT also be used for behavioral advertising purposes or be linked to data used for such purposes, as KSP's Basic Safety Rules do not presently allow for behavioral advertising, even with prior parental consent. *See definition of the term "support for internal operations" under Section 312.2 of Revised COPPA Rule.* Therefore, it is imperative that you confirm that your third party providers are not linking your internal support data with behavioral advertising data.

[72] In other words, once the purposes for collecting the personal information have been fulfilled, the information should be deleted or anonymized. Deletion means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business. *See definition of the term "delete" under Section 312.2 of Revised COPPA Rule.*

[73] Reasonable measures must be taken to protect the information from unauthorized access during the deletion/destruction process. *See Section 312.10 of Revised COPPA Rule.* For paper records (such as signed parental consent forms), this process might require destruction of the records via shredding, pulverizing, or other similar method. For electronic records, this process might entail deleting or anonymizing the information so it is no longer retrievable or readable. *Also see FN 72 above.*

FOOTNOTES FOR SECTION 10

[74] A COPPA-compliant privacy policy is only needed for sites or services that collect some form of personal information from children or that enable children to share personal information with others. However, even when no personal information is collected or shared from children, it is still recommended that you have a privacy policy to state that fact alone and to describe your practices regarding other features (such as the use of web cookies to track non-personal data). You may also have a legal obligation to post a privacy policy under other laws or regulations.

[75] The children's privacy policy can be a sub-section within a broader or more general privacy policy, but only so long as there is a direct link to the children's section from the top of that policy (e.g., table of contents' link).

[76] To be considered "prominent", the link to the privacy policy must be clearly labeled and easily noticeable (*see Section 312.4(d) of Revised COPPA Rule).* This can be achieved either by making the link distinguishable from other surrounding links (such as by making it a larger font size, all CAPS, different color, and/or contrasting background) or by creating a separate eye-catching icon or button for the policy. A small, non-prominent link placed in the global footer of the site or service (although a good idea to cover every page) would not be sufficient.

[77] The privacy policy link must be displayed on the home page of the site or service (or the home page of the children's section of the site/service), and preferably toward the top of the screen (i.e., within initial viewing and no down-scrolling). For mobile apps, the link must be provided on the app's promotion page (i.e., the description page on the relevant app store), as well as on the app's landing screen or menu screen. In addition, a privacy policy link must be provided on every screen where personal information is requested from a child, within close proximity to the fields requesting such information. *See Section 312.4(d) of Revised COPPA Rule.* All links to the policy, wherever offered, should immediately present the policy content, and not require multiple clicks or additional navigation.

[78] The privacy policy must contain the following information *(see Section 312.4(d)(1)-(3) of Revised COPPA Rule*):

- **Contact Information.** Full contact information for the company operating the site or service, including name, address, telephone number, and e-mail address. Also, if applicable, full contact information for any third party companies (such as third party service providers, joint sponsors/operators, third party plug-ins, etc.) that may be collecting personal information *through* your site or service. If you, as the primary owner of the site or service, agree to handle all inquiries related to data collection occurring on or through your site/service (including any data collection by third party features), then only the names of those third parties (not their full contact information) would need to be listed in your policy. (Note, however, that if a third party provider is only collecting and processing a persistent identifier and no other personal information for internal-support related activities (*see FN 56 above for a list of acceptable*

internal support activities), then you would not have to list the name of that third party within your privacy policy. An example of such a third party provider may be a third party analytics provider.)

- **Information Collection Practices.** A description of the types of personal information the site or service collects from children, and whether the site or service enables children to share personal information publicly or with other users (such as through a chat room, community area, or other feature).
- **Information Use Practices.** A description of how the operator of the site or service uses personal information collected from children (e.g., marketing, personalization, to access to special content or features, account maintenance, etc.).
- **Information Sharing Practices.** A statement of whether the operator shares personal information collected from children with third parties, and if so, which types of third parties (e.g., vendors, joint sponsors, etc.).
- **Parental Access Rights.** A statement that parents can review their child's personal information or request that their child's information be deleted or no longer collected or used. The policy must also tell parents how they can exercise these rights (e.g., by providing a link to the parental dashboard area or displaying a contact email address).

[Note: KSP offers a free policy template you can use to help craft a customized policy that meets these requirements and is easy for parents to read and understand. For a copy of this policy, please contact your KSP representative. If you need to craft a mobile-friendly privacy policy, you can consider using this free Policy Maker tool from PrivacyChoice.]

[79] The policy should be written in plain language (not hard-to-understand legalese), should fully describe the practices of the site or service, and should be its own document. It should NOT be bundled or blended together with a terms-of-use document or other legal document. It should also be free of advertisements, promotional materials, or other distracting content. *See Section 312.4(a) of Revised COPPA Rule.*

FOOTNOTES FOR SECTION 11

[80] Material violations may include severe or repeated violations of these Certification Rules or other significant breaches of consumer safety or privacy. This will be determined on a case-by-case basis in the sole discretion of KSP.

[81] The appropriate disciplinary measures for a material violation will be determined on a case-by-case basis in KSP's sole discretion. Factors considered will include the severity of the violation, including (among other things) the number of affected children, the amount and type of data involved, whether personal information was shared publicly or with third parties, and any harm that may have resulted from the violation.

In addition to and separate from enforcement imposed by KSP, the Federal Trade Commission has its own authority to bring enforcement actions against COPPA violators, including enforcement against kidSAFE+ members who are out of compliance with these Certification Rules. It is essential therefore that you keep KSP apprised of all changes to your product features, especially if they affect the collection or handling of children's personal information. *Also see Rule 11(d) of these Certification Rules.*

[82] In addition to being notified about changes in your parental consent techniques so we can help verify your continued compliance, the Revised COPPA Rule allows for FTC-approved safe harbor providers to review and approve new methods of parental consent not currently enumerated under COPPA, provided that such techniques meet the COPPA standard of reliability (i.e., they are "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent"). *See Section 312.5(b)(3) of Revised COPPA Rule.*

ADDENDUM:

Full Text of Revised COPPA Rule

V. Revised Rule

List of Subjects in 16 CFR Part 312

Children, Communications, Consumer Protection, Electronic Mail, E-mail, Internet, Online Service, Privacy, Record Retention, Safety, Science and Technology, Trade Practices, Website, Youth.

Accordingly, for the reasons stated above, the Federal Trade Commission revises Part 312 of Title 16 of the Code of Federal Regulations to read as follows:

PART 312 – CHILDREN'S ONLINE PRIVACY PROTECTION RULE

Sec.

AUTHORITY: 15 U.S.C. 6501-6508

§ 312.1 Scope of regulations in this part.

This part implements the Children's Online Privacy Protection Act of 1998, (15 U.S.C. 6501, et seq.,) which prohibits 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.

§ 312.2 Definitions.

Child means an individual under the age of 13.

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

(a) Requesting, prompting, or encouraging a child to submit personal information online;

(b) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it 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; or

(c) Passive tracking of a child online.

Commission means the Federal Trade Commission.

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

Disclose or disclosure means, with respect to personal information:

(a) The 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; and

(b) 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 electronic mail service; a message board; or a chat room.

Federal agency means an agency, as that term is defined in Section 551(1) of title 5, United States Code.

Internet means 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 means 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 means 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 for commercial purposes involving commerce:

(a) Among the several States or with 1 or more foreign nations;

(b) In any territory of the United States or in the District of Columbia, or between any such territory and

(1) Another such territory, or

(2) Any State or foreign nation; or

(c) Between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

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.

Person means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

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

(a) A first and last name;

(b) A home or other physical address including street name and name of a city or town;

(c) Online contact information as defined in this section;

(d) A screen or user name where it functions in the same manner as online contact information, as defined in this section;

(e) A telephone number;

(f) A Social Security number;

(g) A persistent identifier that can be used to recognize a user over time and across different websites or online services. Such 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;

(h) A photograph, video, or audio file where such file contains a child's image or voice;

(i) Geolocation information sufficient to identify street name and name of a city or town; or

(j) 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 means the sharing, selling, renting, or transfer of personal information to any third party.

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

(a) maintain or analyze the functioning of the website or online service;

(b) perform network communications;

(c) authenticate users of, or personalize the content on, the website or online service;

(d) serve contextual advertising on the website or online service or cap the frequency of advertising;

(e) protect the security or integrity of the user, website, or online service;

(f) ensure legal or regulatory compliance; or

(g) fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4);

so long as the information collected for the activities listed in paragraphs (a)-(g) 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 means any person who is not:

(a) An operator with respect to the collection or maintenance of personal information on the website or online service; or

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

(a) Receives notice of the operator's personal information collection, use, and disclosure practices; and

(b) Authorizes any collection, use, and/or disclosure of the personal information.

Website or online service directed to children means a commercial website or online service, or portion thereof, that is targeted to children.

(a) In determining whether a website or online service, or a portion thereof, is directed to children, the Commission will consider its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.

(b) A website or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another website or online service directed to children.

(c) A website or online service that is directed to children under the criteria set forth in (a) above, but that does not target children as its primary audience, shall not be deemed directed to children if it: (i) does not collect personal information from any visitor prior to collecting age information; and (ii) prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of this part.

(d) A website or online service shall not be deemed directed to children solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

§ 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).

§ 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 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 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 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 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 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.

§ 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.

(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 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).

(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 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, 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.

§ 312.6 Right of parent to review personal information provided by a child.

(a) Upon request of a parent whose child has provided personal 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.

§ 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.

§ 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.

§ 312.9 Enforcement.

Subject to §§ 6503 and 6505 of the Children's Online Privacy Protection Act of 1998, a violation of a regulation prescribed under section 6502 (a) of this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under Section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

§ 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.

§ 312.11 Safe harbor programs.

(a) *In general.* Industry groups or other persons may apply to the Commission for approval of self-regulatory program guidelines ("safe harbor programs"). The application shall be filed with the Commission's Office of the Secretary. The Commission will publish in the FEDERAL REGISTER a document seeking public comment on the application. The Commission shall issue a written determination within 180 days of the filing of the application.

(b) *Criteria for approval of self-regulatory program guidelines.* Proposed safe harbor programs must demonstrate that they meet the following performance standards:

(1) Program requirements that ensure operators subject to the self-regulatory program guidelines ("subject operators") provide substantially the same or greater protections for children as those contained in §§ 312.2 through 312.8, and 312.10.

(2) An effective, mandatory mechanism for the independent assessment of subject operators' compliance with the self-regulatory program guidelines. At a minimum, this mechanism must include a comprehensive review by the safe harbor program, to be conducted not less than annually, of each subject operator's information policies, practices, and representations. The assessment

mechanism required under this paragraph can be provided by an independent enforcement program, such as a seal program.

(3) Disciplinary actions for subject operators' non-compliance with self- regulatory program guidelines. This performance standard may be satisfied by:

(i) Mandatory, public reporting of any action taken against subject operators by the industry group issuing the self-regulatory guidelines;

(ii) Consumer redress;

(iii) Voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the self- regulatory guidelines;

(iv) Referral to the Commission of operators who engage in a pattern or practice of violating the self-regulatory guidelines; or

(v) Any other equally effective action.

(c) *Request for Commission approval of self-regulatory program guidelines.* A proposed safe harbor program's request for approval shall be accompanied by the following:

(1) A detailed explanation of the applicant's business model, and the technological capabilities and mechanisms that will be used for initial and continuing assessment of subject operators' fitness for membership in the safe harbor program;

(2) A copy of the full text of the guidelines for which approval is sought and any accompanying commentary;

(3) A comparison of each provision of §§ 312.2 through 312.8, and 312.10 with the corresponding provisions of the guidelines; and

(4) A statement explaining:

(i) how the self-regulatory program guidelines, including the applicable assessment mechanisms, meet the requirements of this part; and

(ii) how the assessment mechanisms and compliance consequences required under paragraphs (b)(2) and (b)(3) provide effective enforcement of the requirements of this part.

(d) *Reporting and recordkeeping requirements.* Approved safe harbor programs shall:

(1) By July 1, 2014, and annually thereafter, submit a report to the Commission containing, at a minimum, an aggregated summary of the results of the independent assessments conducted under paragraph (b)(2), a description of any disciplinary action taken against any subject operator under paragraph (b)(3), and a description of any approvals of member operators' use of a parental consent mechanism, pursuant to § 312.5(b)(4);

(2) Promptly respond to Commission requests for additional information; and

(3) Maintain for a period not less than three years, and upon request make available to the Commission for inspection and copying:

(i) Consumer complaints alleging violations of the guidelines by subject operators;

(ii) Records of disciplinary actions taken against subject operators; and

(iii) Results of the independent assessments of subject operators' compliance required under paragraph (b)(2).

(e) *Post-approval modifications to self-regulatory program guidelines.* Approved safe harbor programs must submit proposed changes to their guidelines for review and approval by the Commission in the manner required for initial approval of guidelines under paragraph (c)(2). The statement required under paragraph (c)(4) must describe how the proposed changes affect existing provisions of the guidelines.

(f) *Revocation of approval of self-regulatory program guidelines.* The Commission reserves the right to revoke any approval granted under this section if at any time it determines that the approved self-regulatory program guidelines or their implementation do not meet the requirements of this part. Safe harbor programs that were approved prior to the publication of the Final Rule amendments must, by March 1, 2013, submit proposed modifications to their guidelines that would bring them into compliance with such amendments, or their approval shall be revoked.

(g) *Operators' participation in a safe harbor program.* An operator will be deemed to be in compliance with the requirements of §§ 312.2 through 312.8, and 312.10 if that operator complies with Commission-approved safe harbor program guidelines. In considering whether to initiate an investigation or bring an enforcement action against a subject operator for violations of this part, the Commission will take into account the history of the subject operator's participation in the safe harbor program, whether the subject operator has taken action to remedy such non-compliance, and whether the operator's non- compliance resulted in any one of the disciplinary actions set forth in paragraph (b)(3).

§ 312.12 Voluntary Commission Approval Processes.

(a) *Parental consent methods.* An interested party may file a written request for Commission approval of parental consent methods not currently enumerated in §312.5(b). To be considered for approval, a party must provide a detailed description of the proposed parental consent methods, together with an analysis of how the methods meet § 312.5(b)(1). The request shall be filed with the Commission's Office of the Secretary. The Commission will publish in the FEDERAL REGISTER a document seeking public comment on the request. The Commission shall issue a written determination within 120 days of the filing of the request; and

(b) *Support for internal operations of the website or online service.* An interested party may file a written request for Commission approval of additional activities to be included within the definition of support for internal operations. To be considered for approval, a party must provide a detailed justification why such activities should be deemed support for internal operations, and an analysis of their potential effects on children's online privacy. The request shall be filed with the Commission's Office of the Secretary. The Commission will publish in the FEDERAL REGISTER a document seeking public comment on the request. The Commission shall issue a written determination within 120 days of the filing of the request.

§ 312.13 Severability.

The provisions of this part are separate and severable from one another. If any provision is stayed or determined to be invalid, it is the Commission's intention that the remaining provisions shall continue in effect.