

PART III

Side-by-Side Comparison of Each Provision of 16 CFR Part 312 Requirements With i-SAFE Harbor Guideline Requirements

16 CFR PART 312 REQUIREMENTS	Corresponding Guideline Requirement(s) in the i-SAFE Harbor Information Privacy Program
<p>§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</p> <p>Provide Notice on the website or online of what information it collects from children, how it uses such information, and disclosure practices for such information;</p> <p>Obtain verifiable parental consent prior to any collection, use, an/or disclosure of personal information;</p> <p>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;</p> <p>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; and</p> <p>Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.</p>	<p>i-SAFE Harbor Participant/Licensees must prominently display a link that is clearly labeled Privacy Policy or such similar notice that links the parent and/or child to a description of the of the Participant/Licensee’s information collection, use and/or disclosure practices.</p> <p>i-SAFE Harbor Participant/Licensees must make reasonable efforts to ensure that a parent of a child receives notice of the organization’s information collection, use and disclosure practices with regard to children. This includes any material change in the disclosure practices to which the parent previously consented. [NOTE: Participant/Licensees operating Web sites that allow for two-way communications may elect to participate in LEVEL THREE of i-SAFE Harbor by providing a two-process age verification solution. This solution can be implemented using a digital ID and another solution approved by i-SAFE Harbor.] All Participant/Licensees must obtain verifiable parental consent before any collection, use or disclosure of personal information from children unless permitted to collect the child’s name or email address as per one of the exceptions to prior verifiable parental consent set forth in § 312.5 (c) of the Final Rule.</p> <p>i-SAFE Harbor Participant/Licensees must provide a mechanism to access and review their child’s personal information.</p> <p>i-SAFE Harbor Participant/Licensees must not condition a child’s participation in an activity to get the child to disclose more personal information than is reasonable necessary to participate in such activity. [NOTE: i-SAFE Harbor Participant/Licensees that operate Web sites that directly market to children or allow third-party advertising on their site must conform to the CARU self-regulatory program for children’s advertising.]</p> <p>i-SAFE Harbor Participant/Licensees must establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information. i-SAFE Harbor will provide Participant/Licensees with a universally recognized emblem designating their Web site as a safe site.</p>

§312.4 Notice

Notice/Disclosure of Information

Requirement #1: Notice/Disclosure of Information

i-SAFE Harbor Participant/Licensees that collect personal information from children 12 years old or younger must post a prominent link that is clearly labeled *Privacy Policy* or such similar notice that links the children to a description of the Participant/Licensee information collection, use and disclosure practices.

The *Privacy Policy* link must be placed in a clear and prominent place and manner on the homepage of the Participant/Licensee's Web site (or online service) and at each area where personal information is collected from children – and in close proximity to the requests for personal information in each such area.

Privacy Policies must be clear and understandable and should not contain unrelated, contradictory or confusing material. *Privacy Policies* must describe the following information:

Participant/Licensee Contact Information: i-SAFE Harbor Participant/Licensees must include their complete contact information. Such information must include the name mailing address, telephone number, and e-mail address. In cases where more than one company is responsible for a Web site, the Participant/Licensee may choose to respond to all inquiries from parents concerning the Participant/Licensee's *Privacy Policy*, provided that the names of all persons or companies collecting personal information through the Web site are listed.

Types of Personal Information Collected: i-SAFE Harbor Participant/Licensees must describe the types of personal information collected and whether the personal information is collected directly or passively.

Use of Personal Information: i-SAFE Harbor Participant/Licensees must describe how personal information is used.

Disclosure of Personal Information: i-SAFE Harbor Participant/Licensees must state whether personal information is disclosed to third parties. If the Participant/Licensee does disclose personal information, the Participant/Licensee must: 1) describe the types of business in which such third parties are engaged and the general purposes for which the information is used; 2) whether the third parties have agreed to maintain the confidentiality, security and integrity of the personal information they obtain from the Participant/Licensee; and 3) that parents have the option to consent to the collection and use of their children's personal information without consenting to the disclosure of that information to third parties.

Control Over Personal Information: i-SAFE Harbor Participant/Licensees must state in their *Privacy Policy* the choices available to parents and children regarding how a child's personal information is collected and used.

Restrictions on Information Collection: i-SAFE Harbor Participant/Licensees must state they are prohibited from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

Access to Information: i-SAFE Harbor Participant/Licensees must state that parents can review their child's personal information, update their child's information, have such information deleted, and refuse to permit further collection or use of their child's information. Participant/Licensees also must describe the procedures parents must follow to access their child's personal information.

Queries/Complaints: i-SAFE Harbor Participant/Licensees must state in their *Privacy Policy* where parents or children can address any queries or complaints they have concerning the Participant/Licensee's Web site information practices.

Requirement #2: Direct Notice to Parents

i-SAFE Harbor Participant/Licensees must make reasonable efforts to ensure parents receive notice of the Participant/Licensee's information collection, use and disclosure practices with regard to their children, including notice of any material change in the collection, use or disclosure practices to which a parent had previously consented.

Direct notices to parents must contain the following information:

A. Privacy Policy Information: i-SAFE Harbor Participant/Licensees must include all of the information that is necessary to meet Requirement #1 above.

B. Purpose is to Collect Information: i-SAFE Harbor Participant/Licensees must affirmatively state they wish to collect personal information from the parent's child.

C. Parental Consent Required: i-SAFE Harbor Participant/Licensees must affirmatively state that the parent's consent is required for the collection, use or disclosure of their child's personal information. Participant/Licensees also must provide the method by which parents may give such consent.

Except for certain circumstances (i.e., exceptions) described in Requirement #3(C) below, i-SAFE Harbor Participant/Licensees must meet the requirements described above and obtain prior verifiable parental consent before they are allowed to collect personal information from children.

§312.5 Verifiable Parental Consent

As defined in §312.3

Requirement #3: Prior Verifiable Parental Consent

A. Generally, i-SAFE Harbor Participant/Licensees must obtain verifiable parental consent before any collection, use or disclosure of personal information from children. Participant/Licensees also must obtain such consent when there is any material change in the collection, use or disclosure practices to which a parent has previously consented.

B. Methods for Obtaining Prior Verifiable Parental Consent: Any method to obtain prior verifiable parental consent must be reasonably calculated, in light of the available technology, to ensure that the person providing consent is the child's parent.

1. **WHEN PERSONAL INFORMATION IS MADE PUBLICLY AVAILABLE** the methods to obtain prior verifiable parental consent include: 1) providing a consent form to be signed by the parent and returned to the i-SAFE Harbor Participant/Licensee by postal mail or facsimile; 2) requiring the parent to use a credit card in connection with a transaction; 3) requiring the parent to send an e-mail containing the parent's digital signature; 4) having a parent call a toll-free telephone number staffed by trained personnel; or 5) obtaining an e-mail with a PIN or password acquired through one of the four (4) verification methods above.

2. **WHEN PERSONAL INFORMATION IS USED ONLY FOR INTERNAL PURPOSES** (i.e., the personal information will not be disclosed to third parties or made publicly available) the methods to obtain prior verifiable parental consent include the 5 methods listed in paragraph B.1. above and by the "email plus" method. The "email plus" method allows Participant/Licensees to request (in the direct notice to parents) that the parent provide consent in an email message AND, after receiving the parent's email consent, then confirming that it was, in fact, the parent who provided consent by taking the following additional (the "plus") steps:

- Requesting in the Participant/Licensee's initial email seeking consent that the parent include a phone or fax number or mailing address in the reply email, so that Participant/Licensees can follow up to confirm consent via telephone, fax, or postal mail; or
- After a reasonable time delay, sending another email to the parent to confirm consent. In this confirmatory email, Participant/Licensees should include all the original information contained in the direct notice, inform the parent that he or she can revoke the consent, and inform the parent how to revoke the consent.

GENERAL AUDIENCE AND TEEN WEB SITES:
Although a Participant/Licensee may intend their Web site to be for adult and/or teen visitors/users, the need for verifiable parental consent always is triggered (i.e., *Section 312.5* of the Rule applies) when operators of general audience Web sites have actual knowledge that a particular visitor is a child. If an i-SAFE Harbor Participant/Licensee knows that a particular visitor to their Web

site is a child, then the Rule must be followed with respect to that child. A Participant/Licensee can identify which visitors are ages 12 or younger, for example, by asking for age (or birth date) information at any point/place (on the site) where visitors/users can enter/provide personal information (i.e., “age-screen”). Participant/Licensees that choose to use age-screening to ensure personal information of children age 12 or younger is not collected, used or disclosed without prior verifiable parental consent should:

- Design age collection input screens in a manner that does not encourage children to provide a false age in order to gain access to the Participant/Licensee Web site;
- Ask age information in a neutral manner (e.g., a system that allows a user to freely enter month, day, and year of birth – but NOT just birth year and NOT a check box labeled “I am older than age 12”) at the point where the Web site invites visitors to provide personal information or to create a log-in user ID;
- Employ either temporary or permanent cookies to prevent children from “back-buttoning” to change their age in order to circumvent the requirement for verifiable parental consent or to obtain access to the site via, for example, an “entry point or gate.”
- Not encourage children to falsify their age information by stating, for example, that visitors age 12 or younger cannot participate on the Participant/Licensee Web site or should ask their parents before participating.

Upon entering age/birth date information that indicates the individual is a child age 12 or younger, an i-SAFE Harbor Participant/Licensee has several options, which include:

- Collecting the child’s parents’ contact information (e.g., email addresses) to provide direct notice and implement COPPA’s verifiable parental consent requirements; or,
- Configuring the Participant/Licensee data system to automatically delete personal information of visitors/users age 12 or younger, and direct them to content, if available, that does not involve collection or disclosure of personal information; or
- Considering whether the situation falls into one of the five (5) exceptions to the requirement of prior verifiable parental consent and act strictly in accord with the constraints of an applicable exception.

CHILDREN AND TEEN AUDIENCE WEB SITES:

Where an i-SAFE Harbor Participant/Licensee Web site is directed to children and teens and does not age-screen, the i-SAFE Harbor Participant/Licensee must assume a site visitor is a child

age 12 or younger and obtain prior verifiable consent from the child's parent before collecting, using or disclosing the child's personal information.

Finally, even though prior verifiable parental consent is required under most situations before an i-SAFE Harbor Participant/Licensee is permitted to collect, use or disclose a child's personal information, there are a limited number exceptions in which an i-SAFE Harbor Participant/Licensee is permitted to collect a child's first name or online contact information before obtaining consent from the child's parent. In such circumstances, i-SAFE Harbor Participant/Licensees must comply with paragraph VII.A of Guideline Requirement #2, which describes the five (5) exceptions to prior verifiable parental consent and is consistent with §312.5(c) of the Final Rule.

Consistent with §312.5 of the Final Rule, i-SAFE Harbor Participant/Licensees also are required to give parents the option to consent to the collection and use of their child's personal information without consenting to disclosure of that information to third parties. **NOTE:** In the case of social networking sites, chat rooms, message boards and other similar online services, where sharing of personal information is part of the nature of such sites, the Rule does not require operators to give parents the choice to allow them to collect and use their children's personal information but not disclose it to third parties (i.e., because public disclosure of information is integral to such Web sites' operations). Therefore, i-SAFE Harbor Participant/Licensees who operate social networking sites, chat rooms, message boards and similar online services, must clearly disclose their Web sites' information collection and disclosure practices in their *privacy policy* and *direct notice to parents* so that parents understand their consent to collection equals consent to disclosure (i.e., because of the very nature of social networking sites, chat rooms, message boards, etc.) and can make an informed decision.

C. Exceptions to Prior Verifiable Parental Consent:
Even though prior verifiable parental consent is required under most situations before an i-SAFE Harbor Participant/Licensee is permitted to collect, use or disclose a child's personal information, there are a limited number of exceptions where a Participant/Licensee will be allowed to collect a child's first name or online contact information before obtaining consent from the child's parent. The exceptions to prior verifiable parental consent are as follows:

- **Required Parental Consent** – i-SAFE Harbor Participant/Licensees may collect the name or online contact information of a parent to be used for the sole purpose of obtaining parental consent. If a Participant/Licensee has not obtained parental consent after a reasonable time (i.e., from the date the information was collected), the Participant/Licensee must delete such information from its records. Participant/Licensees that collect the name or online contact information from a child under this exception must provide direct notice to the parent. The direct notice must include all *Privacy Policy* information [See Requirement #2(A) above] and

notify the parent the i-SAFE Harbor Participant/Licensee has collected their name and email address to respond to and obtain consent from the parent. If the Participant/Licensee has not obtained parental consent after a reasonable time from the date the information is collected, the i-SAFE Harbor Participant/Licensee must delete such information from its records.

- ***One-Time Request*** – i-SAFE Harbor

Participant/Licensees may collect the online contact information of child (e.g., email address) for the sole purpose of responding directly, on a one-time basis, to a specific request from the child. Participant/Licensees that collect the online contact information from a child under this exception must not use the information to re-contact the child after the initial response and must delete the child's contact information. *Direct notice is not required under this exception.*

- ***Multiple Requests*** – i-SAFE Harbor

Participant/Licensees may collect the online contact information from a child to be used to respond directly more than once to a specific request from the child so long as the information is not used for any other purpose. Participant/Licensees that obtain the online contact information from a child under this exception must provide direct notice to the parent. The direct notice must: 1) include all *Privacy Policy* information [See Requirement 2(A) above]; 2) notify the parent that the Participant/Licensee has collected their child's online contact information in order to respond to their child's request; 3) explain the nature and intended use of the information; 4) inform the parent they may request the Participant/Licensee make no further use of the information and that such information be deleted; 5) describe the procedures by which the parent can refuse to allow further contact and information collection from their child; and 6) explain that if the parent does not opt-out, the i-SAFE Harbor Participant/Licensee may use the information for the purposes stated in the direct notice. The direct notice to the parent must be sent after the initial response and before making any additional response to their child.

- ***Child Safety*** – i-SAFE Harbor Participant/Licensees may collect a child's first name or online contact information to the extent reasonably necessary to protect the safety of a child participant on the Web site where the Participant/Licensee used reasonable efforts to provide notice to the parent. The information collected by the i-SAFE Harbor Participant/Licensee under this exception must be used for the sole purpose of protecting the child's safety, must not be used to re-contact the child or for any other purpose than for the purpose stated in this exception and must not be disclosed by the i-SAFE Harbor Participant/Licensee on its Web site. The direct notice must: 1) include all *Privacy Policy* information [See Requirement #2(A) above]; 2) notify the parent that the

	<p>Participant/Licensee has collected their child’s online contact information to protect the safety of their child participating on the Web site; 3) inform the parent they may refuse to permit the use of the information and may require its deletion, and inform them how they can have the information deleted; and, 4) explain that if the parent does not opt-out, the i-SAFE Harbor Participant/Licensee may use the information for the purposes stated in the direct notice.</p> <ul style="list-style-type: none"> • Additional Safety Concerns – i-SAFE Harbor Participant/Licensees may collect a child’s first name or online contact information to protect the security or integrity of its Web site, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or investigations on matters related to public safety so long as the information is not used for any other purpose. Direct notice is not required under this exception.
<p>§312.6 Right of Parent to Review Personal Information Provided by Child</p> <p>As defined in §312.3</p>	<p>Requirement #4: <u>Access and Review</u></p> <p>i-SAFE Harbor Participant/Licensees must provide parents with the ability to access and review their child’s personal information. Parental review and access must consist of: 1) a description of the specific types of personal information collected from their child; 2) the opportunity at any time to refuse to permit the Participant/Licensee further using or collecting their child’s personal information; and 3) the ability to direct the Participant/Licensee to delete their child’s personal information from the Participant/Licensee’s records.</p> <p>In addition to providing the ability for a parent to access and review their child’s personal information, i-SAFE Harbor Participant/Licensees must take reasonable steps to ensure the individual requesting access is the parent of the child. Acceptable steps for authenticating the identity of the parent online include a username and password unique to the parent or, if access is requested over the telephone, asking a series of questions about which only a parent of the child would have knowledge (e.g., parent’s name, mailing address or e-mail address; or the child’s name, e-mail address, etc.).</p>
<p>§312.7 Prohibition Against Conditioning a Child’s Participation on Collection of Personal Information</p> <p>As defined in §312.3</p>	<p>Requirement #5: <u>Restrictions on Information Collection</u></p> <p>i-SAFE Harbor Participant/Licensees are prohibited from conditioning a child’s participation in an activity upon the child disclosing more personal information than is reasonably necessary to participate in such activity.</p>

§312.8 Confidentiality, Security, and Integrity of Personal Information

As defined in § 312.3

Requirement #6: Confidentiality, Security and Integrity of Information

i-SAFE Harbor Participant/Licensees must establish and maintain reasonable procedures to protect the confidentiality, security and integrity of personal information collected from children.

§312.9 Enforcement

Violation of COPPA would 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).

Requirement #7: Compliance/Enforcement

A. Program Representatives: i-SAFE Harbor Participant/Licensees must appoint a program representative for their Web site(s). The program representative shall be the individual responsible for overseeing the Web site's compliance with i-SAFE Harbor Guideline Requirements. Program representatives shall be given the authority to investigate, in a timely manner, all inquiries concerning the Web site's *Privacy Policy* and information practices.

B. Initial and Annual Self-Evaluation: i-SAFE Harbor Participant/Licensees must conduct a self-evaluation (i.e., assessment) of their Web site information collection, use and disclosure practices (i.e. the *CAC*). Each Participant/Licensee is required to complete and attest to the accuracy of the statements made in the *CAC* self-evaluation form concerning their information practices. When i-SAFE receives a *CAC*, an i-SAFE Harbor representative will independently review the respective Web site's posted *Privacy Policy*, information practices and the *CAC* self-evaluation form to verify compliance with i-SAFE Harbor Guideline Requirements. If the Participant/Licensee's Web site is determined to be in full compliance with i-SAFE Harbor Guideline Requirements, it will then be listed as a Participant/Licensee in the i-SAFE Harbor program. i-SAFE Harbor Participant/Licensees are required to complete and submit an updated *CAC* self-evaluation form on an annual basis to ensure their Web site's information practices remain consistent with their posted *Privacy Policy* and i-SAFE Harbor Guideline Requirements.

C. Compliance Monitoring: i-SAFE Harbor Participant/Licensees must submit to monitoring reviews of their Web site's information practices. The purpose of monitoring reviews is to ensure that a Participant/Licensee's *Privacy Policy* is consistent with its Web site information practices. Monitoring reviews also allow i-SAFE to verify the Participant/Licensee's Web site complies with i-SAFE Harbor Guideline Requirements at all times. Compliance monitoring reviews (announced and/or unannounced) may be conducted quarterly or semi-annually or annually. If i-SAFE determines that a violation of i-SAFE Harbor

Guideline Requirements has occurred, the Participant/Licensee is informed of the violation and also the corrective actions that must be taken to bring the Participant/Licensee's Web site into compliance. Failure to take corrective action(s) can result in a number of consequences, including removal from the i-SAFE Harbor program and referral to the appropriate governmental agency.

D. Consumer Complaints/Monitoring: i-SAFE Harbor Participant/Licensees must provide parents and children with reasonable and effective means to submit and attempt to resolve complaints about i-SAFE Harbor Participant/Licensee's information practices (i.e., internal complaint/dispute resolution). i-SAFE Harbor also offers parents and children the opportunity to submit complaints about any i-SAFE Harbor Participant/Licensee directly to i-SAFE via third-party complaint/dispute resolution. In third-party complaint/dispute resolutions, an i-SAFE Harbor representative responds to all complaints immediately and i-SAFE Harbor Participant/Licensees must agree to work with i-SAFE representatives to cooperatively resolve all complaints submitted to i-SAFE Harbor for third-party complaint/dispute resolution. To support both Participant/Licensee internal complaint/dispute resolution processes and third-party complaint/dispute resolution processes, Participant/Licensees must maintain records for a period of three (3) years of all complaints, concerns or inquiries received about its Web site and any responses to consumers addressing such complaints or concerns.

E. License Agreement: i-SAFE Harbor Participant/Licensees must execute an i-SAFE Harbor Participant License Agreement (**PLA**). As part of this License Agreement, Participant/Licensees agree to comply with i-SAFE Harbor Guideline Requirements at all times. In the event a Participant/Licensee fails to meet any of its obligations under the **PLA**, such failure would constitute a material breach of the License Agreement and the i-SAFE Harbor Participant/Licensee's membership in the i-SAFE Harbor program may be terminated.