FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Complying with COPPA: Frequently Asked Questions

TAGS: Privacy and Security | Children's Privacy

RELATED RULE: Children's Online Privacy Protection Rule ("COPPA")

Need resources on the Children's Online Privacy Protection Rule? These revised FAQs from the FTC can help keep your company COPPA compliant.

A GUIDE FOR BUSINESS AND PARENTS AND SMALL ENTITY COMPLIANCE GUIDE

(March 20, 2015: FAQ M.1, M.4, and M.5 revised. FAQ M.6 deleted)

The following FAQs are intended to supplement the compliance materials available on the FTC website. In addition, you may send questions or comments to the FTC staff's COPPA mailbox, CoppaHotLine@ftc.gov. This document represents the views of FTC staff and is not binding on the Commission. To view the Rule and compliance materials, go to the FTC's COPPA page for businesses. This document serves as a small entity compliance guide pursuant to the Small Business Regulatory Enforcement Fairness Act.

Some FAQs refer to a type of document called a Statement of Basis and Purpose. A Statement of Basis and Purpose is a document an agency issues when it promulgates or amends a rule, explaining the rule's provisions and addressing comments received in the rulemaking process. A Statement of Basis and Purpose was issued when the COPPA Rule was promulgated in 1999, and another Statement of Basis and Purpose was issued when the Rule was revised in 2012.

A. GENERAL QUESTIONS ABOUT THE COPPA RULE

1. What is the Children's Online Privacy Protection Rule?

Congress enacted the Children's Online Privacy Protection Act (COPPA) in 1998. COPPA required the Federal Trade Commission to issue and enforce regulations concerning children's online privacy. The Commission's original COPPA Rule became effective on April 21, 2000. The Commission issued an amended Rule on December 19, 2012. The amended Rule took effect on July 1, 2013.

The primary goal of COPPA is to place parents in control over what information is collected from their young children online. The Rule was designed to protect children under age 13 while accounting for the dynamic nature of the Internet. The Rule applies to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children, and operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. The Rule also applies to websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children. Operators covered by the Rule must:

1. Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children;
2. Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information online from children;
3. Give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties (unless disclosure is integral to the site or service, in which case, this must be made clear to parents);
4. Provide parents access to their child's personal information to review and/or have the information deleted;
5. Give parents the opportunity to prevent further use or online collection of a child's personal information;
6. Maintain the confidentiality, security, and integrity of information they collect from children, including by taking reasonable steps to release such information only to parties capable of maintaining its confidentiality and security; and
7. Retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect

against its unauthorized access or use.

2. Who is covered by COPPA?

The Rule applies to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children. It also applies to operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. The Rule also applies to websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children.

3. What is Personal Information?

The amended Rule defines personal information to include:

First and last name;

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

Online contact information;

A screen or user name that functions as online contact information;

A telephone number;

A social security number;

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

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

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

Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described above.

4. When does the amended Rule go into effect? What should I do about information I collected from children prior to the effective date that was not considered personal under the original Rule but now is considered personal information under the amended Rule?

The amended Rule, which goes into effect on July 1, 2013, added four new categories of information to the definition of personal information. The amended Rule of course applies to any personal information that is collected after the effective date of the Rule. Below we address, for each new category of personal information, an operator's obligations regarding use or disclosure of previously collected information that will be deemed personal information once the amended Rule goes into effect:

If you have collected **geolocation information** and have not obtained parental consent, you must do so immediately. Although geolocation information is now a stand-alone category within the definition of personal information, the Commission has made clear that this was simply a clarification of the 1999 Rule. The definition of personal information from the 1999 Rule already covered any geolocation information that provides information precise enough to identify the name of a street and city or town. Therefore, operators are required to obtain parental consent prior to collecting such geolocation information, regardless of when such data is collected.

If you have collected **photos or videos containing a child's image or audio files with a child's voice from a child** prior to the effective date of the amended Rule, you do not need to obtain parental consent. This is consistent with the Commission's statement contained in the 1999 Statement of Basis and Purpose for the COPPA Rule that operators need not seek parental consent for information collected prior to the effective date of the Rule. However, as a best practice, staff recommends that entities either discontinue the use or disclosure of such information after the effective date of the amended Rule or, if possible, obtain parental consent.

Under the original Rule, a **screen or user name** was only considered personal information if it revealed an individual's email address. Under the amended Rule, a screen or user name is personal information where it functions in the same manner as online contact information, which includes not only an email address, but any other "substantially similar identifier that permits direct contact with a person online." As with photos, videos, and audio, any newly-covered screen or user name collected prior to the effective date of the amended Rule is not covered by COPPA, although we encourage you as a best practice to obtain parental consent if possible. A previously-collected screen or user name is covered, however, if the operator associates new information with it after the effective date of the amended Rule.

Persistent identifiers were covered by the original Rule only where they were combined with individually identifiable information. Under the amended Rule, a persistent identifier is covered where it can be used to recognize a user over time and across different websites or online services. Consistent with the above, operators need not seek parental consent for these newly-covered persistent identifiers if they were collected prior to the effective date of the Rule. However, if after the effective date of the amended Rule an operator continues to collect, or associates new information with, such a persistent identifier, such as information about a child's activities on its website or online service, this collection of information about the child's activities triggers COPPA. In this situation, the operator is required to obtain prior parental consent unless such collection falls under an exception, such as for support for the internal operations of the website or online service.

5. I don't collect any of the newly-covered types of personal information. Other than the changes to the definition of personal information, in what ways is the new Rule different?

As discussed in additional FAQs below, the amendments to the Rule help to ensure that COPPA continues to meet its originally stated goals to minimize the collection of personal information from children and create a safer, more secure online experience for them, even as online technologies, and children's uses of such technologies, evolve. The final Rule amendments, among other things:

Modify the definition of "operator" to make clear that the Rule covers an operator of a child-directed site or service where it integrates outside services, such as plug-ins or advertising networks, that collect personal information from its visitors. The definition of "Web site or online service directed to children" was also amended to clarify that the Rule covers a plug-in or ad network when it has actual knowledge that it is collecting personal information through a child-directed website or online service and to allow a subset of child-directed sites and services to differentiate among users;

Streamline and clarify the direct notice requirements to ensure that key information is presented to parents in a succinct ''just-in-time'' notice;

Expand the non-exhaustive list of acceptable methods for obtaining prior verifiable parental consent;

Create new exceptions to the Rule's notice and consent requirements;

Strengthen data security protections;

Require reasonable data retention and deletion procedures;

Strengthen the Commission's oversight of self-regulatory safe harbor programs; and

Institute voluntary pre-approval mechanisms for new consent methods and for activities that support the internal operations of a website or online service.

6. Where can I find information about COPPA?

The FTC has a comprehensive website which provides information to the public on a variety of agency activities. The Children's Privacy section includes a variety of materials regarding COPPA, including all proposed and final Rules, public comments received by the Commission in the course of its rulemakings, guides for businesses, parents, and teachers, information about the Commission-approved COPPA safe harbor programs, and FTC cases brought to enforce COPPA. Many of the educational materials on the FTC website also are available in hard copy free of charge at ftc.gov/bulkorder.

7. What should I do if I have questions about the COPPA Rule?

The first thing you should do is read the FTC's Children's Privacy guidance materials. If, after reviewing the FTC's online materials, you continue to have specific COPPA questions, please send an email to our COPPA hotline at CoppaHotLine@ftc.gov.

8. What should I do if I have a complaint about someone violating the COPPA Rule?

You may fill out a complaint form online. You also may call our toll free telephone number, (877) FTC-HELP, to submit your complaint to a live operator.

9. I know that COPPA doesn't just apply to websites, but also to "online services." What types of online services does COPPA apply to?

COPPA applies to personal information collected online by operators of both websites and online services. The term "online service" broadly covers any service available over the Internet, or that connects to the Internet or a wide-area network. Examples of online services include services that allow users to play network-connected games, engage in social networking activities, purchase goods or services online, receive online advertisements, or interact with other online content or services. Mobile applications that connect to the Internet, Internet-enabled gaming platforms, voice-over-Internet protocol services, and Internet-enabled location-based services also are online services covered by COPPA.

10. Does COPPA apply to information *about* children collected online from parents or other adults?

No. COPPA only applies to personal information collected online *from* children, including personal information about themselves, their parents, friends, or other persons. However, the Commission's 1999 Statement of Basis and Purpose notes that the Commission expects that operators will keep confidential *any* information obtained from parents in the course of obtaining parental consent or providing for parental access pursuant to COPPA. *See* 64 Fed. Reg. 59888, 59902 n.213.

11. Why does COPPA apply only to children under 13? What about protecting the online privacy of teens?

In enacting the Children's Online Privacy Protection Act, Congress determined to apply the statute's protections only to children under 13, recognizing that younger children are particularly vulnerable to overreaching by marketers and may not understand the safety and privacy issues created by the online collection of personal information.

Although COPPA does not apply to teenagers, the FTC is concerned about teen privacy and does believe that strong, more flexible, protections may be appropriate for this age group. *See* FTC Report: Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (Mar. 2012), at 29, 60. The FTC also has issued a number of guidance documents for teens and their parents. These educational materials are available at www.OnguardOnline.gov.

12. I know the COPPA Rule is triggered by the collection of personal information from children, but the information I collect at my site or service is voluntary, not mandatory. Does COPPA still apply?

Yes. The Rule governs the online collection of personal information from children by a covered operator, even if children volunteer the information or are not required by the operator to input the information to participate on the webssite or service. The Rule also covers operators that allow children publicly to post personal information. Finally, as the FTC made clear in the amended Rule, the passive tracking of children's personal information through a persistent identifier, and not just its active collection, also is covered by COPPA. *See* 16 C.F.R. § 312.2 (definition of "collection").

13. Will the COPPA Rule keep my child from accessing pornography?

No. COPPA is meant to give parents control over the online collection, use, or disclosure of personal information from children, and was not designed to protect children from viewing particular types of content wherever they might go online. If you are concerned about your children accessing online pornography or other inappropriate materials, you may want to consider a filtering program or an Internet Service Provider that offers tools to help screen out or restrict access to such material. Information about such tools is available at organizations such as www.getnetwise.org and www.staysafeonline.org, and from manufacturers of several operating systems.

14. Will the amended COPPA Rule prevent children from lying about their age to register for general audience sites or online services whose terms of service prohibit their participation?

No. COPPA covers operators of general audience websites or online services only where such operators have actual knowledge that a child under age 13 is the person providing personal information. The Rule does not require operators to ask the age of visitors. However, an operator of a general audience site or service that chooses to screen its users for age in a neutral fashion may rely on the age information its users enter, even if that age information is not accurate. In some circumstances, this may mean that children are able to register on a site or service in violation of the operator's Terms of Service. If, however, the operator later determines that a particular user is a child under age 13, COPPA's

notice and parental consent requirements will be triggered.

B. COPPA ENFORCEMENT

1. How does the FTC enforce the Rule?

Information about the FTC's COPPA enforcement actions can be found by clicking on the Case Highlights link in the FTC's Business Center. Parents, consumer groups, industry members, and others that believe an operator is violating COPPA may submit complaints to the FTC through the FTC's website, www.ftc.gov, or toll free number, (877) FTC-HELP.

2. What are the penalties for violating the Rule?

A court can hold operators who violate the Rule liable for civil penalties of up to $16,000 per violation. The amount of civil penalties a court assesses may turn on a number of factors, including the egregiousness of the violations, whether the operator has previously violated the Rule, the number of children involved, the amount and type of personal information collected, how the information was used, whether it was shared with third parties, and the size of the company. Information about the FTC's COPPA enforcement actions, including the amounts of civil penalties obtained, can be found by clicking on the Case Highlights link in the FTC's Business Center.

3. Can the states or other federal government agencies enforce COPPA?

Yes. COPPA gives states and certain federal agencies authority to enforce compliance with respect to entities over which they have jurisdiction. In the past, Texas and New Jersey have brought COPPA enforcement actions. *See* https://www.oag.state.tx.us/oagnews/release.php?id=2288 (Dec. 2007), and http://www.nj.gov/oag/newsreleases12/pr20120606a.html (June 2012). In addition, certain federal agencies, such as the Office of the Comptroller of the Currency and the Department of Transportation, are responsible for handling COPPA compliance for the specific industries they regulate.

4. What should I do if my website or app doesn't comply with the Rule?

First, until you get your website or online service into compliance, you must stop collecting, disclosing, or using personal information from children under age 13.

Second, carefully review your information practices and your online privacy policy. In conducting your review, look closely at what information you collect, how you collect it, how you use it, whether the information is necessary for the activities on your site or online service, whether you have adequate mechanisms for providing parents with notice and obtaining verifiable consent, whether you have adequate methods for parents to review and delete their children's information, and whether you employ adequate data security, retention, and deletion practices.

Educational materials aimed at operators of websites and online services are available in the Children's Privacy Section of the FTC's Business Center. *See also* Marketing Your Mobile App: Get it Right From the Start. These materials can provide you with helpful guidance. You might also choose to consult with one of the Commission-approved COPPA Safe Harbor Programs or seek the advice of counsel.

5. Are websites and online services operated by nonprofit organizations subject to the Rule?

COPPA expressly states that the law applies to commercial websites and online services and not to nonprofit entities that otherwise would be exempt from coverage under Section 5 of the FTC Act. In general, because many types of nonprofit entities are not subject to Section 5 of the FTC Act, these entities are not subject to the Rule. However, nonprofit entities that operate for the profit of their commercial members may be subject to the Rule. *See FTC v. California Dental Association*, 526 U.S. 756 (1999). Although nonprofit entities generally are not subject to COPPA, the FTC encourages such entities to post privacy policies online and to provide COPPA's protections to their child visitors.

6. Does COPPA apply to websites and online services operated by the Federal Government?

As a matter of federal policy, all websites and online services operated by the Federal Government and contractors operating on behalf of federal agencies must comply with the standards set forth in COPPA. *See* OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 2003).

7. The Internet is a global medium. Do websites and online services developed and run abroad have to comply with the Rule?

Foreign-based websites and online services must comply with COPPA if they are directed to children in the United States, or if they knowingly collect personal information from children in the U.S. The law's definition of "operator" includes foreign-based websites and online services that are involved in commerce in the United States or its territories. As a related matter, U.S.-based sites and services that collect information from foreign children also are subject to COPPA.

C. PRIVACY POLICIES AND DIRECT NOTICES TO PARENTS

1. My child-directed website doesn't collect any personal information. Do I still need to post a privacy policy online?

COPPA applies only to those websites and online services that collect, use, or disclose personal information from children. However, the FTC recommends that all websites and online services – particularly those directed to children – post privacy policies online so visitors can easily learn about the operator's information practices. *See* Mobile Apps for Kids: Disclosures Still Not Making the Grade (Dec. 2012) and Mobile Apps for Kids: Current Privacy Disclosures are Dis*app*ointing (Feb. 2012).

2. What information must I include in my online privacy policy?

Section 312.4(d) of the amended Rule identifies the information that must be disclosed in your online privacy policy. While the original Rule required operators to provide extensive categories of information in their online privacy notices,

the amended Rule now takes a shorter, more streamlined approach to cover the information collection and use practices most critical to parents. Under the amended Rule, the online notice must state the following three categories of information:

> The name, address, telephone number, and email address of all operators collecting or maintaining personal information through the site or service (or, after listing all such operators, provide the contact information for one that will handle all inquiries from parents);
>
> A description of what information the operator collects from children, including whether the operator enables children to make their personal information publicly available, how the operator uses such information, and the operator's disclosure practices for such information; and
>
> That the parent can review or have deleted the child's personal information and refuse to permit its further collection or use, and state the procedures for doing so. See 16 C.F.R. § 312.4(d) ("notice on the Web site or online service").

By streamlining the Rule's online notice requirements, the Commission hopes to encourage operators to provide clear, concise descriptions of their information practices, which may have the added benefit of being easier to read on smaller screens (e.g., those on smartphones or other Internet-enabled mobile devices).

3. May I include promotional materials in my privacy policy?

No. The Rule requires that privacy policies must be "clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials." *See* 16 C.F.R. § 312.4(a) ("General principles of notice").

4. I already have a privacy policy for my children's app. Do I have to change it to comply with the amended COPPA Rule?

It depends. The amended Rule expands the types of information that are considered "personal." *See* 16 C.F.R. § 312.2 (definition of personal information). Therefore, you should examine your information collection practices to determine whether you are collecting information from children that is now considered personal under the Rule, and that now may require you to notify parents and obtain their consent. In addition, you should review the amended Rule's requirements for the form and content of privacy notices to make sure that your direct notices (*see* FAQ C.11 below) and online privacy policies comply (*see* FAQ C.2 above). *See* 16 C.F.R. § 312.4(b) and (d).

5. Do I have to list the names and contact information of all the operators collecting information at my website? This will make my online privacy policy very long and confusing.

The amended Rule retains the requirement that, if there are multiple operators collecting information through your site (including via plug-ins), you may list the name, address, phone number, and email address of one operator who will respond to all inquiries from parents regarding all of the operators' privacy policies and use of children's information, as long as the names of all the operators are also listed in this online notice. *See* 16 C.F.R. § 312.4(d)(1). If you wish to keep your online privacy policy simple, you may include a clear and prominent link in the privacy policy to the complete list of operators, as opposed to listing every operator in the policy itself. You must ensure, however, that your privacy policy signals parents to, and enables them easily to access, this list of operators. *See* .com Disclosures: How to Make Effective Disclosures in Digital Advertising (Mar. 2013), at ii.

6. Do I have to disclose in my privacy policy and direct notices to parents the collection of "cookies," "GUIDs," "IP addresses," or other passive information collection technologies on or through my site?

The amended Rule defines "personal information" to include identifiers, such as a customer number held in a cookie, an IP address, a processor or device serial number, or a unique device identifier that can be used to recognize a user over time and across different websites or online services, even where such identifier is not paired with other items of personal information. Therefore, you will need to disclose in your privacy policy (*see* FAQ C.2), and in your direct notice to parents (*see* FAQ C.11), your collection, use or disclosure of such persistent identifiers unless (1) you collect no other "personal information," and (2) such persistent identifiers are collected on or through your site or service solely for the purpose of providing "support for the internal operations" of your site or service. For more detailed information about activities considered support for internal operations, *see* FAQs I.5-8, below.

7. Where should I post links to my privacy policy?

The amended Rule requires that the operator post a clearly and prominently labeled link to the online privacy policy on the home or landing page or screen of the website or online service, and at each area of the site or service where personal information is collected from children. This link must be in close proximity to the requests for information in each such area. 16 C.F.R. § 312.4(d).

In addition, an operator of a general audience website or online service that has a separate children's area must post a link to its notice of information practices with regard to children on the home or landing page or screen of the children's area. *See* 16 C.F.R. § 312.4(d).

8. Is it okay for the link to my privacy policy to be located at the bottom of the home page of my website?

The amended Rule states that the "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 Web site or online service, *and,* at each area of the Web site or online service where personal information is collected from children." 16 C.F.R. § 312.4(d). In the 1999 Statement of Basis and Purpose, the Commission explained that "'clear and prominent' means that the link must stand out and be noticeable to the site's visitors through use, for example, of a larger font size in a different color on a contrasting background. The Commission does not consider 'clear and prominent' a link that is in small print at the bottom of the home page, or a link that is indistinguishable from a number of other, adjacent links." *See* 64 Fed. Reg. 59888, 59894. A link that is at the bottom of the page *may* be acceptable if the manner in which it is presented makes it clear and prominent.

9. I have an app directed to children. Do I need to make sure that my privacy policy is included in the app store, at the point of purchase or download?

The amended Rule does not mandate that a privacy policy be posted at the point of purchase; rather, the Rule requires that it be posted on the home or landing screen. However, there is a substantial benefit in providing greater transparency about the data practices and interactive features of child-directed apps at the point of purchase and we

encourage it as a best practice. In fact, the FTC Staff Report, Mobile Apps for Kids: Disclosures Still Not Making the Grade (Dec. 2012) notes that "information provided prior to download is most useful in parents' decision-making since, once an app is downloaded, the parent already may have paid for the app..." *See* p. 7. Further, if a child-directed app were designed to collect personal information as soon as it is downloaded, it would be necessary to provide the direct notice and obtain verifiable consent at the point of purchase or to insert a landing page where a parent can receive notice and give consent before the download is complete.

10. I operate a general audience website that contains a specific children's section. May I post a single privacy policy for the entire site that combines information about my children's and general information practices, or must I have a separate privacy policy for children's data?

In the 1999 Statement of Basis and Purpose, the Commission noted that "operators are free to combine the privacy policies into one document, as long as the link for the children's policy takes visitors directly to the point in the document where the operator's policies with respect to children are discussed, or it is clearly disclosed at the top of the notice that there is a specific section discussing the operator's information practices with regard to children." *See* 64 Fed. Reg. 59888, 59894 n.98. This advice remains in effect under the amended Rule. Operators should also ensure that the link for the children's portion of the privacy policy appears on the home page or screen of the children's area of the site or service, and at each area where personal information is collected from children. *See* 16 C.F.R. § 312.4(d).

11. I know that the amended Rule made some changes to the direct notice that must be sent to parents before I collect personal information from children. What are those changes?

The Rule requires operators to 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 changes to practices to which the parent previously consented. The amended Rule significantly changed the format and content of the information that must be included in an operator's direct notice to parents. The Rule now provides a very detailed roadmap of what information must be included in your direct notice depending upon what personal information is collected and for what purposes.

There are four instances where a direct notice is required or appropriate under the Rule:

1. Where an operator seeks to obtain a parent's verifiable consent prior to the collection, use, or disclosure of a child's personal information. In this case, the direct notice must:

    State 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;

    State 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;

    Set forth 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;

    Contain a hyperlink to the operator's online notice of its information practices (i.e., its privacy policy);

    Provide the means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and

State 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. *See* 16 C.F.R. § 312.4(c)(1).

2. Where an operator voluntarily seeks to provide notice to a parent of a child's online activities that do not involve the collection, use or disclosure of personal information. In this case, the direct notice must:

   State 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;

   State that the parent's online contact information will not be used or disclosed for any other purpose;

   State 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

   Provide a hyperlink to the operator's online notice of its information practices. *See* 16 C.F.R. § 312.4(c)(2).

3. Where an operator intends to communicate with the child multiple times via the child's online contact information and collects no other information. In this case, the direct notice must:

   State that the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child;

   State 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;

   State 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;

   State 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;

   State 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

   Provide a hyperlink to the operator's online notice of its information practices. *See* 16 C.F.R. § 312.4(c)(3).

4. Where the operator's purpose for collecting a child's and a parent's name and online contact information is to protect a child's safety and the information is not used or disclosed for any other purpose. In this case, the direct notice must:

   State 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;

   State that the information will not be used or disclosed for any purpose unrelated to the child's safety;

   State that the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so;

   State 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

   Provide a hyperlink to the operator's online notice of its information practices. *See* 16 C.F.R. § 312.4(c)(4).

12. When I send a direct notice to parents, may I send them a simple email containing a link to my online privacy policy?

No. As described in FAQ C.11 above, the amended Rule makes clear that the direct notice to parents must contain

certain key information within the four corners of the notice itself, depending on the purpose for which the information is being collected. Therefore, you may not simply link to a separate online notice. Note, however, that in addition to the key information, the amended Rule requires that each direct notice you send also contain a link to your online privacy policy. The intention of these changes is to help ensure that the direct notice functions as an effective "just-in-time" message to parents about an operator's information practices, while also directing parents online to view any additional information contained in the operator's online notice.

13. I have an app directed to children. At what point in the download process should I send parents my direct notice?

Unless one of the limited exceptions applies (*see* FAQ H.2), the Rule requires that you send parents the direct notice prior to the collection of any personal information from the child. The limited exception to this is that you may collect the parent's online contact information for the sole purpose of sending the parent the direct notice. Alternatively, you may provide the direct notice to the parent through other means, such as through the device onto which the app is downloaded, if the mechanisms both (1) provide such notice and obtain the parent's consent before any collection of personal information and (2) are reasonably designed to ensure that it is the parent who receives the notice and provides the consent.

D. WEBSITES AND ONLINE SERVICES DIRECTED TO CHILDREN

1. COPPA applies to websites or online services that are "directed to children." What determines whether or not a website or online service is directed to children?

The amended Rule sets out a number of factors for determining whether a website or online service is directed to children. These include subject matter of the site or service, its visual content, the 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, or whether advertising promoting or appearing on the website or online service is directed to children. The Rule also states that the Commission will consider competent and reliable empirical evidence regarding audience composition, as well as evidence regarding the intended audience of the site or service. *See* 16 C.F.R. § 312.2 (definition of "Web site or online service directed to children," paragraph (1)).

As described in FAQ D.5 below, the amended Rule also considers a website or online service to be "directed to children" where it has actual knowledge that it is collecting personal information directly from users of another website or online service that is directed to children. *See* 16 C.F.R. § 312.2 (definition of "Web site or online service directed to children," paragraph (2)).

2. I run a child-directed app. I would like to screen users so that I only have to get parental consent from children under age 13, not from everyone who uses the app. May I?

It depends. Because of its very nature, in most instances, a website or online service (such as an app) directed to

children must treat all visitors as children and provide COPPA's protections to every such visitor. This means that for the most part, a website or online service directed to children may not screen users for age.

However, the amended Rule provides for a narrow exception for a site or service that may be directed to children under the criteria set forth in FAQ D.1 above, but that does not target children as its *primary* audience. For instance, a child-directed site may target children under age 13, as well as parents or younger teens. An operator of a site or service meeting this standard may age-screen its users if it: (1) does not collect personal information from any visitor prior to collecting age information, and (2) prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the amended Rule's notice and parental consent provisions. *See* 16 C.F.R. § 312.2 (definition of "Web site or online service directed to children," paragraph (3)). Importantly, as an operator of a website or online service directed to children, you may not block children from participating in the website or online service (*see* FAQ D.4 below).

3. What evidence would I need to demonstrate whether children under age 13 are or are not the "primary target audience" for my website?

As the operator, you should carefully analyze who your intended audience is, the actual audience, and in many instances, the likely audience for your site or service. In making these determinations, you should keep in mind the factors for a "Web site or online service directed to children" contained in paragraph (1) of 16 C.F.R. § 312.2. *See* FAQ D.1 above. You may also get a better sense of your site or service once it has been in operation, and may need to make some changes accordingly.

4. I run a site that I believe may fall within the FTC's sub-category of a website directed to children but where it is acceptable to age-screen users. Can I age-screen and completely block users who identify as being under age 13 from participating in any aspect of my site?

No. If your site falls within the definition of a "Web site or online service directed to children" as set forth in paragraph (1) of 16 C.F.R. § 312.2, then you may not block children from participating altogether, even if you do not intend children to be your primary target audience. Instead, what the amended Rule now permits you to do is to use an age screen in order to differentiate between your child and non-child users. You may decide to offer different activities, or functions, to your users depending upon age, but you may not altogether prohibit children from participating in a child-directed site or service.

5. [Now at FAQ D.10]

6. Am I required to inform third parties that my website or online service is directed to children? Even if I am not required to do so, how can I do this? If I signal the nature of my site or service, will this protect me from liability under COPPA?

The amended Rule does not require you to inform third parties of the child-directed nature of your site or service, and doing so, without more, will not relieve you of your obligations under COPPA. Remember, you are responsible for the collection of personal information from your users, no matter who is doing the collection; therefore, you will need to do more than simply identify yourself to third parties. As a child-directed property, absent an exception under the amended Rule (*see* FAQ H.2 below), you must: (1) not collect or allow any other entity to collect personal information from your visitors; or (2) provide notice and obtain prior parental consent before collecting or allowing any entity to collect personal information from your visitors, as well as provide all of the other COPPA protections. In addition, Commission staff recommends that operators of child-directed websites or services signal their status to third parties and you may arrange with the third party collecting the personal information to provide adequate COPPA protections.

7. I want to run ads on my child-directed websites and apps. What do I need to know to make sure that I am complying with COPPA?

There are a number of questions you must find answers to before you enter into an arrangement with any entity to serve advertising to run on your child-directed sites and services. These include:

> Is there a way to control the type of advertising that appears on the sites and services? (*e.g.*, can you stipulate and contract only for contextual advertising, and can you prohibit behavioral advertising or retargeting?)
>
> What categories of information will be collected from users on the sites and services in connection with the ads they are served? Will persistent identifiers be collected for purposes other than support for internal operations? Will geolocation information be collected in connection with the ads served?

You should make informed decisions before you permit advertising to run on your sites and services. Depending on what advertising choices you make, you may be required to notify parents in your online privacy policies and in a direct notice, and obtain verifiable parental consent, before you permit advertising to occur. Remember that the amended Rule holds you liable for the collection of information that occurs on or through your sites and services, even if you yourself do not engage in such collection.

8. I have no idea what information the third parties whose content I have embedded in my kids' app might collect from my users. Do I need to know this information?

Yes. As the operator of a child-directed app, you must conduct an inquiry into the information collection practices of every third party that can collect information via your app. You need to determine each third party's information collection practices so that you can make an informed decision as to whether its presence on your app will require you to give parents notice and obtain their consent prior to their collection of personal information from children. *See* FAQ D.6 above.

9. I operate a child-directed app that allows kids to make paintings. I don't collect the paintings — they rest on the device — but the app includes buttons for popular email and social media providers that kids can click on within the app. The buttons open the email program or social network, populate it with the painting,

and allow the child to share it along with a message. I don't collect or share any other personal information through the app. Do I have to seek verifiable parental consent?

Yes. The COPPA rule defines "collection" to include requesting, prompting, or encouraging a child to submit personal information online, and enabling a child to make personal information publicly available in identifiable form. In addition, under the COPPA Rule, "disclosure" includes making a child's personal information publicly available in identifiable form through an email service or other means, such as a social network. You must get verifiable parental consent before enabling children to share personal information in this manner, even through third parties on your app. This is true unless an exception applies. (See Section I, Exceptions to Prior Parental Consent). However, in the situation you describe — where a child can email a painting and a message or post content on his or her social networking page through your app — no exception applies.

10. I operate an advertising network service. Under what circumstances will I be held to have "actual knowledge" that I have collected personal information directly from users of another website or online service directed to children?

The circumstances under which you will be deemed to have acquired "actual knowledge" that you have collected personal information directly from users of a child-directed site or service will depend a lot on the particular facts of your situation. In the 2012 Statement of Basis and Purpose, the Commission set forth two cases where it believes that the actual knowledge standard will likely be met:

1. where a child-directed content provider (which is strictly liable for any collection) directly communicates the child-directed nature of its content to you, the ad network; or

2. where a representative of your ad network recognizes the child-directed nature of the content.

Under the first scenario, any direct communications that the child-directed provider has with you that indicate the child-directed nature of its content would give rise to actual knowledge. In addition, if a formal industry standard or convention is developed through which a site or service could signal its child-directed status to you, that would give rise to actual knowledge. Under the second scenario, whether a particular individual can obtain actual knowledge on behalf of your business depends on the facts. Prominently disclosing on your site or service methods by which individuals can contact your business with COPPA information – such as: 1) contact information for designated individuals, 2) a specific phone number, and/or 3) an online form or email address – will reduce the likelihood that you would be deemed to have gained actual knowledge through other employees. (See also FAQ D.12 below).

11. I operate an ad network. I receive a list of websites from a parents' organization, advocacy group or someone else, which says that the websites are child-directed. Does this give me actual knowledge of the child-directed nature of these sites?

It's unlikely the receipt of a list of purportedly child-directed websites alone would constitute actual knowledge. You would have no duty to investigate. It's possible, however, that you will receive screenshots or other forms of concrete information that do give you actual knowledge that the website is directed at children. If you receive information and are uncertain whether the site is child-directed, you may ordinarily rely on a specific affirmative representation from the

website operator that its content is not child-directed. For this purpose, a website operator would not be deemed to have provided a specific affirmative representation if it merely accepts a standard provision in your Terms of Service stating that, by incorporating your code, the first party agrees that it is not child directed.

12. I operate an ad network and am considering participating in a system in which first-party sites could signal their child-directed status to me, such as by explicit signaling from the embedding webpage to ad networks. I understand that I would have "actual knowledge" if I collect information from users on a first-party site that has signaled its child-directed status. Are there any benefits to me if I participate in such a system?

Such a system could provide more certainty for you. If the system requires the first-party site to affirmatively certify whether it is "child-directed" or "not child-directed," and the site signals that it is "not child-directed," you may ordinarily rely on such a representation. Such reliance is advisable, however, only if first parties affirmatively signal that their sites or services are "not child-directed." You could not set that option for them as the default.

Remember, though, that you may still be faced with screenshots or other concrete information that gives you actual knowledge of the child-directed nature of the website despite a contradictory representation by the site. If, however, such information is inconclusive, you may ordinarily continue to rely on a specific affirmative representation made through a system that meets the criteria above.

E. PHOTOS, VIDEOS, AND AUDIO RECORDINGS

1. I run a moderated website that is directed to children and I prescreen all children's submissions in order to delete personal information before postings go live. Do I have to get parental consent if I allow children to post photos of themselves but no other personal information?

Yes. The amended Rule considers photos, videos, and audio recordings that contain a child's image or voice to be personal information. This means that operators covered by COPPA must either (i) prescreen and delete from children's submissions any photos, videos, or audio recordings of themselves or other children or (ii), first give parents notice and obtain their consent prior to permitting children to upload any photos, videos, or audio recordings of themselves or other children.

2. I want to offer a child-directed app. The app would allow children to upload pictures of their favorite pets or places. I do not ask children to provide their email addresses or their names, or really any personal information for that matter. How does

COPPA apply to me?

COPPA applies to photos, videos, and audio files that contain children's images or voices. It also applies to geolocation data contained in these files sufficient to identify street name and name of city or town. Finally, it applies to any persistent identifiers collected via the children's upload of their photos. Therefore, in order to offer an app without parental notice and consent, the operator must take the following steps

1. Pre-screen the children's photos in order to delete any that depict images of children or to delete the applicable portion of the photo, if possible. The operator must also remove any other personal information, for example, geolocation metadata, contained in the photos prior to posting them through the app. Note that if an operator does not pre-screen, then it may be subject to civil penalties under COPPA if any personal information is collected from children without the operator first notifying parents and obtaining their consent; and

2. Ensure that any persistent identifiers are used only to support the internal operations of the app (as that term is defined in the Rule) and are not used or disclosed to contact a specific individual or for any other purpose.

3. Do I have to get parental consent if first I blur images in the children's photos so that you cannot see any facial features when the pictures go live on my site?

An operator of a site directed to children does not need to notify parents or obtain their consent if it blurs the facial features of children in photos before posting them on its website. *See* 2012 Statement of Basis and Purpose, 78 Fed. Reg. 3972, 3982 n.123. The same goes for a site that has actual knowledge it has collected the photos from children. Before posting such photos, however, the operator must also remove any other personal information they contain, such as geolocation metadata, and ensure that it is not using or disclosing persistent identifiers collected from children in a manner that violates the amended Rule.

4. Does the amended Rule prohibit adults, such as parents, grandparents, teachers, or coaches from uploading photos of children?

COPPA only covers information collected online from children. It does not cover information collected from adults that may pertain to children. Thus, COPPA is not triggered by an adult uploading photos of children on a general audience site or in the non-child directed portion of a mixed-audience website.

However, operators of websites or online services that are primarily directed to children (as defined by the Rule) must assume that the person uploading a photo is a child and they must design their systems either to: (1) give notice and obtain prior parental consent, (2) remove any child images and metadata prior to posting, or (3) create a special area for posting by adults, if that is the intention.

5. My app is directed to children. A child can upload photos into the app and manipulate and decorate the photos in different ways, but the app does not transmit any personal information (photos or otherwise) from the child's device. Am I "collecting" personal information because the child is interacting with a photo stored on

the device?

No. You are not collecting personal information simply because your app interacts with personal information that is stored on the device and is never transmitted.

F. GEOLOCATION DATA

1. I automatically collect geolocation information from users of my children's app, but I do not use this information for anything. Am I responsible for notifying parents and getting their consent to such collection?

Yes. COPPA covers the collection of geolocation information, not just its use or disclosure.

2. What if I give my users a choice to turn off geolocation information? Do I still have to notify parents and get prior parental consent?

COPPA is designed to notify parents and give them the choice to consent. Therefore, it is not sufficient to provide such notification and choice to the child user of a website or service. If the operator intends to collect geolocation information, the operator will be responsible for notifying parents and obtaining their consent prior to such collection.

3. The amended Rule covers "geolocation information sufficient to identify street name and name of city or town." What if my children's app only collects coarse geolocation information, tantamount to collecting a ZIP code but nothing more specific?

COPPA does not require an operator to notify parents and obtain their consent before collecting the type of coarse geolocation services described. However, the operator should be quite certain that, in all instances, the geolocation information it collects is more general than that sufficient to identify street name and name of city or town.

4. The geolocation information I collect through my app provides coordinate numbers. It does not specifically identify a street name and name of city or town. Do I have to notify parents and get their consent in this instance?

COPPA covers the collection of geolocation information "sufficient" to identify street name and name of city or town. It does not require the actual address identification of such information at the time of collection. One example where COPPA would be triggered is where an app takes the user's longitude and latitude coordinates and translates them to a precise location on a map.

G. GENERAL AUDIENCE, TEEN, AND MIXED-AUDIENCE SITES OR SERVICES

1. Am I responsible if children lie about their age during the registration process on my general audience website?

The Rule does not require operators of general audience sites to investigate the ages of visitors to their sites or services. *See* 1999 Statement of Basis and Purpose, 64 Fed. Reg. 59888, 59892. However, operators will be held to have acquired actual knowledge of having collected personal information from a child where, for example, they later learn of a child's age or grade from a concerned parent who has learned that his child is participating on the site or service.

2. I have an online service that is intended for teenagers. How does COPPA affect me?

Although you may intend to operate a "teen service," in reality, your site may attract a substantial number of children under 13, and thus may be considered to be a "Web site or online service directed to children" under the Rule. Just as the Commission considers several factors in determining whether a site or service is directed to children, you too should consider your service's subject matter, visual content, character choices, music, and language, among other things. If your service targets children as one of its audiences – even if children are not the primary audience – then your service is "directed to children."

In circumstances where children are not the primary audience of your child-directed service, the amended Rule allows you to employ an age screen in order to provide COPPA's protections to only those visitors who indicate they are under age 13. Note that sites or services directed to children cannot use the age screen to block children under age 13. *See* FAQ D.2 above. Once you identify child visitors, you may choose to:

1. Collect parents' online contact information to provide direct notice in order to obtain parents' consent to your information collection, use and disclosure practices; or
2. Direct child visitors to content that does not involve the collection, use, or disclosure of personal information.

3. Can I block children under 13 from my general audience website or online service?

Yes. COPPA does not require you to permit children under age 13 to participate in your general audience website or online service, and you may block children from participating if you so choose. By contrast, you may not block children from participating in a website or online service that is directed to children as defined by the Rule. *See* FAQ D.2 above.

If you choose to block children under 13 on your general audience site or service, you should take care to design your age screen in a manner that does not encourage children to falsify their ages to gain access to your site or service. Ask age information in a neutral manner at the point at which you invite visitors to provide personal information or to create a user ID.

In designing a neutral age-screening mechanism, you should consider:

Making sure the data entry point allows users to enter their age accurately. An example of a neutral age-screen would be a system that allows a user freely to enter month, day, and year of birth. A site that includes a drop-

down menu that only permits users to enter birth years making them 13 or older, would not be considered a neutral age-screening mechanism since children cannot enter their correct ages on that site.

Avoiding encouraging children to falsify their age information, for example, by stating that visitors under 13 cannot participate or should ask their parents before participating. In addition, simply including a check box stating, "I am over 12 years old" would not be considered a neutral age-screening mechanism.

In addition, consistent with long standing Commission advice, FTC staff recommends using a cookie to prevent children from back-buttoning to enter a different age. Note that if you ask participants to enter age information, and then you fail either to screen out children under age 13 or to obtain their parents' consent to collecting these children's personal information, you may be liable for violating COPPA. *See, e.g.,* the FTC's COPPA cases against *Path, Inc.*, *Playdom, Inc.* and *Sony BMG Music Entertainment*.

4. I operate a general audience gaming site and do not ask visitors to reveal their ages. I do permit users to submit feedback, comments, or questions by email. What are my responsibilities if I receive a request for an email response from a player who indicates that he is under age 13?

Under the Rule's one-time response exception (16 C.F.R. § 312.5(c)(3)) you are permitted to send a response to the child, via the child's online contact information, without sending notice to the parent or obtaining parental consent. However, you must delete the child's online contact information from your records promptly after you send your response. You may not use the child's online contact information to re-contact the child (or for any other purpose), or disclose the child's online contact information. Note that if you choose not to respond to the child's inquiry, you must still immediately delete the child's personal information from your records. Additionally, such an email may give you actual knowledge that you have collected personal information from a child (*e.g.*, if you had previously collected the child's email address as part of a website registration process). In such a circumstance, you would need to take steps to ensure that you are complying with COPPA, such as obtaining parental consent or immediately deleting any personal information collected from the child.

5. I operate a general audience online service and do not ask visitors to reveal their ages. However, I do permit users to create their own blog pages, and my service has a number of online forums.

(a) What happens if a child registers on my service and posts personal information (*e.g.,* on a comments page) but does not reveal his age anywhere?

The COPPA Rule is not triggered in this scenario. The Rule applies to an operator of a general audience website if it has actual knowledge that a particular visitor is a child. If a child posts personal information on a general audience site or service but does not reveal his age, and if the operator has no other information that would lead it to know that the visitor is a child, then the operator would not be deemed to have acquired "actual knowledge" under the Rule and would not be

subject to the Rule's requirements.

However, even where a child himself has not revealed his age on a site or service, an operator may acquire actual knowledge where it later learns of a child's age – for example, through a report from a concerned parent who has discovered that her child is participating on the site. Where an operator knows that a particular visitor is a child, the operator must either meet COPPA's notice and parental consent requirements or delete the child's information.

(b) What happens if a child posts in a forum and announces her age?

If no one in your organization is aware of the post, then you may not have the requisite actual knowledge under the Rule. However, you may be considered to have actual knowledge where a child announces her age under certain circumstances, for example, if you monitor your posts, if a responsible member of your organization sees the post, or if someone alerts you to the post (*e.g.*, a concerned parent who learns that his child is participating on your site).

H. VERIFIABLE PARENTAL CONSENT

1. When do I have to get verifiable parental consent?

The Rule provides generally that an operator must obtain verifiable parental consent before collecting any personal information from a child, unless the collection fits into one of the Rule's exceptions described in various FAQs herein. *See* 16 C.F.R. § 312.5(c).

2. May I first collect personal information from the child, and then get parental permission to such collection if I do not use the child's information before getting the parent's consent?

As a general rule, operators must get verifiable parental consent before collecting personal information online from children under 13. Certain, limited exceptions let operators collect certain personal information from a child before obtaining parental consent. *See* 16 C.F.R. § 312.5(c). These exceptions include:

Where the sole purpose of collecting the name or online contact information of the parent or child is to provide notice to the parent and obtain parental consent. Note that under this exception, 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;

Where the sole purpose of collecting a parent's online contact information is to provide voluntary notice about the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information. Such information cannot be used or disclosed for any other purpose and the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with appropriate notice;

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;

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. Here, the operator must provide parents with notice and the means to opt out of allowing the site's future contact of the child. In providing such notice, the operator must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives appropriate notice and will not be deemed to have made reasonable efforts where the notice to the parent was unable to be delivered;

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. Here, the operator must make reasonable efforts, taking into consideration available technology, to provide a parent with appropriate notice;

Where the purpose of collecting a child's name and online contact information is to:

Protect the security or integrity of its website or online service;

Take precautions against liability;

Respond to judicial process; or

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;

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 as outlined in FAQ I.5 below; or

Where a third-party operator has actual knowledge that it has a presence on a child-directed site (*e.g.*, through a social widget or plug-in embedded on the site), it collects a persistent identifier and no other personal information from a visitor of the child-directed site, and the third-party operator's previous affirmative interaction with that user confirmed the user was not a child (*e.g.*, an age-gated registration process).

3. I collect personal information from children who use my online service, but I only use the personal information I collect for internal purposes and I never give it to third parties. Do I still need to get parental consent before collecting that information?

It depends. First, you should determine whether the information you collect falls within one of the amended Rule's limited exceptions to parental consent outlined in FAQ H.2 above. If you fall outside of one of those exceptions, you must notify parents and obtain their consent. However, if you only use the information internally, and do not disclose it to third parties or make it publicly available, then you may obtain parental consent through use of the Rule's "email plus" mechanism, as outlined in FAQ H.4 below. *See* 16 C.F.R. § 312.5(b)(2).

4. How do I get parental consent?

You may use any number of methods to obtain verifiable parental consent, as long as the method you choose is reasonably calculated to ensure that the person providing consent is the child's parent. The Rule sets forth several non-

exhaustive options, and you can apply to the FTC for pre-approval of a new consent mechanism, as set out in FAQ H.14 below.

If you are going to disclose children's personal information to third parties, or allow children to make it publicly available (*e.g.*, through a social networking service, online forums, or personal profiles) then you must use a method that is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. Such methods include:

- Providing a consent form to be signed by the parent and returned via U.S. mail, fax, or electronic scan (the "print-and-send" method);
- Requiring the 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;
- Having the parent call a toll-free telephone number staffed by trained personnel, or have the parent connect to trained personnel via video-conference; or
- Verifying a parent's identity by checking a form of government-issued identification against databases of such information, provided that you promptly delete the parent's identification after completing the verification.

If you are going to use children's personal information only for internal purposes – that is, you will not be disclosing the information to third parties or making it publicly available – then you can use any of the above methods or you can use the "email plus" method of parental consent. "Email plus" allows you to request (in the direct notice sent to the parent's online contact address) that the parent indicate consent in a return message. To properly use the email plus method, you must take an additional confirming step after receiving the parent's message (this is the "plus" factor). The confirming step may be:

- Requesting in your initial message to the parent that the parent include a phone or fax number or mailing address in the reply message, so that you can follow up with a confirming phone call, fax or letter to the parent; or
- After a reasonable time delay, sending another message via the parent's online contact information to confirm consent. In this confirmatory message, you 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 do so.

5. I would like to get consent by collecting a credit card or debit card number from the parent, but I don't want to engage in a monetary transaction. Is this ok?

It depends. The general rule is that any parental consent mechanism "must be reasonably calculated, in light of available technology, to ensure that the parent providing consent is the child's parent." The Rule lists several methods that automatically meet this standard, one of which is the use of a credit card, debit card, or other online payment system in connection with a monetary transaction. However, the listed methods aren't exhaustive; you may use other methods as long as they are "reasonably calculated" to ensure that the consent is being provided by the parent. Although collecting a 16-digit credit or debit card number alone would not satisfy this standard, there may be circumstances in which collection of the card number – in conjunction with implementing other safeguards – would suffice. For example, you could supplement the request for credit card information with special questions to which only parents would know the answer and find supplemental ways to contact the parent.

6. I would like to use a credit card or a government-issued identification as a method of parental consent. I am worried,

however, that I will not know whether it is the child's parent or another adult who is submitting identification for consent. Do I need to collect additional information to confirm that, in fact, it is the parent?

No. By providing appropriate notice and obtaining consent in connection with the amended Rule's proper use of a credit card or government identification, the operator will be deemed to fulfill its obligation under the Rule.

7. What do I do if some parents cannot or will not use the consent method I have chosen? For instance, some parents might not have a credit card, or might feel uncomfortable providing government identification information online.

Many operators find it useful to offer a choice of consent methods for those parents who cannot, or will not, use their primary consent mechanism. At the very least, you might consider offering one alternate method that parents might be more comfortable with, such as a print-and-send form.

8. Should I give out passwords or PIN numbers to parents to confirm their identity in any future contact with them?

Once you have notified a parent and obtained verifiable consent, providing a password or a PIN number is a good way to confirm a parent's identity for any future contact you might have with that parent. Remember that if you change your information practices in a material way in the future, you will have to send a new parental notice and obtain an updated consent to the new practices. Obtaining an updated consent may be easier if you have given the parent a password or a PIN number in your initial consent process.

In addition, the Rule requires you to give a parent access to any personal information you have collected from the child. Before you provide that information, you will need to confirm that the person requesting the information is the child's parent. Again, providing the parent a password or a PIN number makes it easier to confirm the parent's identity if the parent requests access to the child's personal information.

9. I know that I must allow parents to consent to my collection and use of their children's information, while giving them the option of prohibiting me from disclosing that information to third parties. Does that mean that if I operate a social networking site, or have chat rooms or message boards, I have to offer the same kind of "choice" about these types of sites as well?

The Rule requires an operator to give parents the option to consent to the collection and use of a child's personal information without consenting to the disclosure of such information to third parties. *See* 16 C.F.R. § 312.5(a)(2). However, an operator must only provide this choice where the disclosure of the information is not inherent in the activity to which the parent is consenting.

You should note that the Rule's definition of "disclosure" is broader than merely "releasing" personal information to third

parties. Under the Rule, "disclosure" includes "[m]aking 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." *See* 16 C.F.R. § 312.2.

In the case of social networking sites, chat rooms, message boards, and other similar online services, sharing personal information is a central feature of the site. Therefore, in these cases, you are not required to give parents the choice to allow you to collect and use their children's personal information, but not disclose it to third parties. However, you must clearly disclose your information collection, use, and disclosure practices in your direct notice and online privacy policy so that parents can make an informed decision about their children's participation in your site or service.

10. I am the developer of an app directed to kids. Can I use a third party, such as one of the app stores, to get parental consent on my behalf?

Yes, as long as you ensure that COPPA requirements are being met. For example, you must make sure that the third party is obtaining consent in a way that is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. The mere entry of an app store account number or password, without other indicia of reliability (e.g., knowledge-based authentication questions or verification of government identification), does not provide sufficient assurance that the person entering the account or password information is the parent, and not the child. You must also provide parents with a direct notice outlining your information collection practices before the parent provides his or her consent.

11. What types of information can I collect to obtain or confirm parental consent? Can I use a parent's mobile phone number to obtain or confirm parental consent?

The Rule permits you to collect the parent's "online contact information," defined as an email address, an IM user identifier, a VOIP identifier, a video chat user identifier, or other substantially similar identifier. A mobile phone number is not online contact information and therefore cannot be collected from the child as part of the consent initiation process. However, once you have connected with the parent via the parent's online contact information, you may request a parent's mobile phone number in order to further communicate with him or her.

12. How long will "email plus" remain an approved form of parental consent?

The amended Rule identifies email plus as an acceptable method for verifiable parental consent where an operator does not "disclose" children's personal information. The Commission has determined that email-plus shall be permanent, just as are the other approved methods for verifiable parental consent.

13. Can I use a third party to carry out my notice and consent obligations for me?

Yes. For instance, several of the Commission-approved COPPA safe harbor programs offer parental notification and consent systems for operators who are members of their programs. In addition, the Commission recognized in the 2012 Statement of Basis and Purpose that these and other common consent mechanisms could benefit operators (especially

smaller ones) and parents if they offer a proper means for providing notice and obtaining verifiable parental consent, as well as ongoing controls for parents to manage their children's accounts. *See* 78 Fed. Reg. 3972, 3989. Remember that, whether or not you use a common consent mechanism to assist in providing notice and obtaining consent, as the operator you are responsible for ensuring that the notice accurately and completely reflects your information collection practices and that the consent mechanism is reasonably designed to reach the parent.

14. Can I apply to the FTC for pre-approval of a new consent mechanism?

Yes. The amended Rule provides a mechanism for interested parties to file a written request for Commission approval of parental consent methods not currently enumerated in 16 C.F.R. § 312.5(b). *See* 16 C.F.R. § 312.12(a).

15. I would like to apply to the FTC for approval of a new method of parental consent that I have developed, but I am concerned about having my trade secrets publicly posted. Is there a way to prevent this?

The Commission recognized this concern in the 2012 Statement of Basis and Purpose, noting that, "just as the Commission has done for COPPA safe harbor applicants, it would permit those entities that voluntarily seek approval of consent mechanisms to seek confidential treatment for those portions of their applications that they believe warrant trade secret protection. In the event an applicant is not comfortable with the Commission's determination as to which materials will be placed on the public record, it will be free to withdraw the proposal from the approval process." *See* 78 Fed. Reg. 3972, 3992.

16. I run an app store, and would like to help app developers that operate on my platform by providing a verifiable parental consent mechanism for them to use. Under what circumstances will this expose me to liability under COPPA?

Because you are not an "operator" under COPPA in this circumstance, you will not be liable under COPPA for failing to investigate the privacy practices of the operators for whom you obtain consent. As the Commission stated in the Statement of Basis and Purpose accompanying the final COPPA Rule, the term "operator" is not intended to encompass platforms, "such as Google Play or the App Store, when such stores merely offer the public access to someone else's child-directed content." At the same time, you should also evaluate your potential liability under Section 5 of the FTC Act. For example, it could be a deceptive practice to misrepresent the level of oversight you provide for a child-directed app.

I. EXCEPTIONS TO PRIOR PARENTAL CONSENT

1. I want to have a contest on my child-directed website. Can I

use the Rule's "one-time contact" exception to prior parental consent?

Yes, if you properly design your contest. You may use the "one time contact" exception if you collect children's online contact information, and only this information, to enter them in the contest, and then only contact such children once when the contest ends to notify them if they have won or lost. At that point, you must delete the online contact information you have collected.

If, however, you expect to contact the children more than one time, you must use the "multiple-contact" exception, for which you must also collect a parent's online contact information and provide parents with direct notice of your information practices and an opportunity to opt out. In either case, the Rule prohibits you from using the children's online contact information for any other purpose, and requires you to ensure the security of the information, which is particularly important if the contest runs for any length of time.

If you wish to collect any information from children online beyond online contact information in connection with contest entries – such as collecting a winner's home address to mail a prize – you must first provide parents with direct notice and obtain verifiable parental consent, as you would for other types of personal information collection beyond online contact information. If you do need to obtain a mailing address and wish to stay within the one-time exception, you may ask the child to provide his parent's online contact information and use that identifier to notify the parent if the child wins the contest. In your prize notification message to the parent, you may ask the parent to provide a home mailing address to ship the prize, or invite the parent to call a telephone number to provide the mailing information.

2. I have a child-directed website that has an "Ask the Author" corner where children can email questions to featured authors. Do I need to provide notice and obtain parental consent?

If you simply answer the child's question and then delete the child's email address (and do not otherwise maintain or store the child's personal information in any form), then you fall into the Rule's "one-time contact" exception and do not need to obtain parental consent.

3. I offer e-cards and the ability for children to forward items of interest to their friends on my child-directed app. Can I take advantage of one of the Rule's exceptions to parental consent or must I notify parents and obtain consent for this activity?

The answer depends on how you design your e-card or forward-to-a-friend system. Any system providing any opportunity to reveal personal information other than the recipient's email address requires you to obtain verifiable consent from the sender's parent (not email plus), and does not fall within one of COPPA's limited exceptions. This means that if your e-card/forward-to-a-friend system permits personal information to be disclosed either in the "from" or "subject" lines, or in the body of the message, then you must notify the sender's parent and obtain verifiable parental consent *before* collecting any personal information from the child.

In order to take advantage of COPPA's "one-time contact exception" for your e-cards, your web form may only collect the recipient's email address (and, if desired, the sender or recipient's first name); you may not collect any other personal information either from the sender or the recipient, including persistent identifiers that track the user over time and across sites. Moreover, in order to meet this one-time contact exception, your e-card system must not allow the sender to enter her full name, her email address, or the recipient's full name. Nor may you allow the sender to freely type messages either in the subject line or in any text fields of the e-card.

Finally, you should send the e-card immediately and automatically delete the recipient's email address immediately after sending. If you choose to retain the recipient's email address until some point in the future (*e.g.*, until the e-card is opened by the recipient, or you allow the sender to indicate a date in the future when the e-card should be sent), then this collection parallels the conditions for the Rule's "multiple contact exception" for obtaining verifiable parental consent. In this scenario, you must collect the sender's parent's email address and provide notice and an opportunity to opt out to the sender's parent *before* the e-card is sent. *See* 1999 Statement of Basis and Purpose, 64 Fed. Reg. 59888, 59902 n.222.

4. I would like to collect email address, but no other personally identifying information, during my website's registration process. I intend to use the email address only for the purpose of providing password reminders to users who register on my site. Do I first have to provide notice and obtain parental consent before collecting a child's email address?

If you plan to retain the child's email address in retrievable form after the initial collection, to be used, for example, to email children reminders of their passwords, then you must provide notice to parents and the opportunity to opt out under the Rule's multiple-contact exception. *See* 16 C.F.R. § 312.5(c)(4).

However, you may collect a child's email address to be used to authenticate the child for purposes of generating a password reminder without first providing parental notice and giving a parent the opportunity to opt out if you meet the following conditions: (1) you do not collect any personal information from the child other than the child's email address; (2) the child cannot disclose any personal information on your website; and (3) you immediately and permanently alter the email address (*e.g.*, through "hashing") such that it can only be used as a password reminder and cannot be reconstructed into its original form or used to contact the child. You should explain this process in a clear and conspicuous manner, both at the point of collection and in your site's online privacy policy, so that your users and their parents are informed about how the email addresses will be used. This will prevent confusion by visitors and others who may otherwise assume that your site is improperly collecting and retaining email addresses without any form of parental notice.

5. What does "support for the internal operations of the Web site or online service" mean?

"Support for the internal operations of the Web site or online service," as defined in 16 C.F.R. 312.2, means activities necessary for the site or service to maintain or analyze its functioning; perform network communications; authenticate users or personalize content; serve contextual advertising or cap the frequency of advertising; protect the security or integrity of the user, website, or online service; ensure legal or regulatory compliance; or fulfill a request of a child as permitted by § 312.5(c)(3) and (4). Persistent identifiers collected for the sole purpose of providing support for the internal operations of the website or online service do not require parental consent, so long as no other personal information is collected and the persistent identifiers are 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.

6. Can both a child-directed website and a third-party plug-in that collect persistent identifiers from users of that child-directed site

rely on the Rule's exception for "support for internal operations"?

Yes. A child-directed site and a third-party plug-in collecting persistent identifiers from users of that child-directed site can both rely upon the Rule's "support for internal operations" exception where the only personal information collected from such users are persistent identifiers for purposes outlined in the "support for internal operations" definition. The persistent identifier information collected by the third-party plug-in may in some instances support only the plug-in's internal operations; in other instances, it may support both its own internal operations and the internal operations of the child-directed site.

7. Does the exception for "support for internal operations" allow me to perform, or retain another party to perform, site analytics?

Yes. Where you, a service provider, or a third party collects persistent identifier information from users of your child-directed site to perform analytics encompassed by the Rule's "support for internal operations" definition, and the information is not used for any other purposes not covered by the support for internal operations definition, then you can rely upon the Rule's exemption from parental and consent.

8. I am an ad network that uses persistent identifiers to personalize advertisements on websites. I know that I operate on a child-directed site, but isn't personalization considered "support for internal operations"?

No. The term "support for internal operations" does not include behavioral advertising. The inclusion of personalization within the definition of support for internal operations was intended to permit operators to maintain *user driven* preferences, such as game scores, or character choices in virtual worlds. "Support for internal operations" does, however, include the collection or use of persistent identifiers in connection with serving contextual advertising on the child-directed site.

9. I have a child-directed app and want to send push notifications. Do I need to get parental consent?

The information you collect from the child's device used to send push notifications is online contact information – it permits you to contact the user outside the confines of your app – and is therefore personal information under the Rule. To the extent the child has specifically requested push notifications, however, you may be able to rely on the "multiple-contact" exception to verifiable parental consent, for which you must also collect a parent's online contact information and provide parents with direct notice of your information practices and an opportunity to opt-out. See FAQ H.2. Importantly, in order to fit within this exception, your push notifications must be reasonably related to the content of your app. If you want to combine this online contact information with other personal information collected from the child, you cannot rely on this exception and must provide parents with direct notice and obtain verifiable parental consent prior to sending push notifications to the child.

10. I have a child-directed website. Can I put a plug-in, such as Facebook Like button, on my site without providing notice and obtaining verifiable parental consent?

In determining whether you must provide notice and obtain verifiable parental consent, you will need to evaluate whether any exceptions apply. Section 312.5(c)(8) of the Rule has an exception to its notice and consent requirements where:

1. a third-party operator only collects a persistent identifier and no other personal information;
2. the user affirmatively interacts with that third-party operator to trigger the collection; and
3. the third-party operator has previously conducted an age-screen of the user, indicating the user is not a child.

If the third-party operator meets all of those requirements, and if your site doesn't collect personal information (except for that covered by an exception), you don't need to provide notice or obtain consent.

This exception doesn't apply to types of plug-ins where the third party collects more information than a persistent identifier — for example, where the third party also collects user comments or other user-generated content. In addition, a child-directed website can't rely on this exception to treat particular visitors as adults and track their activities.

If your inclusion of the plug-in satisfies all the criteria of section 312.5(c)(8) outlined above and/or satisfies another exception to the notice and consent requirements in the Rule (see, for example, the "support for internal operations" exception discussed in FAQ I.5 and I.6 above), you do not have to provide notice and obtain verifiable parental consent.

J. PARENTAL ACCESS TO CHILDREN'S PERSONAL INFORMATION

1. Do I have to keep all information I have ever collected online from a child in case a parent may want to see it in the future?

No. As the Commission noted in the 1999 Statement of Basis and Purpose, "if a parent seeks to review his child's personal information after the operator has deleted it, the operator may simply reply that it no longer has any information concerning that child." *See* 64 Fed. Reg. 59888, 59904.

2. What if, despite my most careful efforts, I mistakenly give out a child's personal information to someone who is not that child's parent or guardian?

The Rule requires you to provide parents with a means of reviewing any personal information you collect online from children. Although the Rule provides that the operator must ensure that the requestor is a parent of the child, it also notes that if you follow reasonable procedures in responding to a request for disclosure of this personal information, you will not be liable under any federal or state law if you mistakenly release a child's personal information to a person other than the parent. *See* 16 C.F.R. § 312.6(a)(3)(i) and (b).

K. DISCLOSURE OF INFORMATION TO THIRD PARTIES

1. If I want to share children's personal information with a service provider or a third party, how should I evaluate whether the security measures that entity has in place are "reasonable" under the Rule?

Before sharing information with such entities, you should determine what the service providers' or third parties' data practices are for maintaining the confidentiality and security of the data and preventing unauthorized access to or use of the information. Your expectations for the treatment of the data should be expressly addressed in any contracts that you have with service providers or third parties. In addition, you must use reasonable means, such as periodic monitoring, to confirm that any service providers or third parties with which you share children's personal information maintain the confidentiality and security of that information.

2. I operate an ad network. I discover three months after the effective date of the Rule that I have been collecting personal information via a child-directed website. What are my obligations regarding personal information I collected after the Rule's effective date, but before I discovered that the information was collected via a child-directed site?

Unless an exception applies, you must provide notice and obtain verifiable parental consent if you: (1) continue to collect new personal information via the website, (2) re-collect personal information you collected before, or (3) use or disclose personal information you know to have come from the child-directed site. With respect to (3), you have to obtain verifiable parental consent before using or disclosing previously-collected data only if you have actual knowledge that you collected it from a child-directed site. In contrast, if, for example, you had converted the data about websites visited into interest categories (e.g., sports enthusiast) and no longer have any indication about where the data originally came from, you can continue to use those interest categories without providing notice or obtaining verifiable parental consent. In addition, if you had collected a persistent identifier from a user on the child-directed website, but have not associated that identifier with the website, you can continue to use the identifier without providing notice or obtaining verifiable parental consent.

With respect to the previously-collected personal information you know came from users of a child-directed site, you must comply with parents' requests under 16 C.F.R. § 312.6, including requests to delete any personal information collected from the child, even if you will not be using or disclosing it. Furthermore, as a best practice you should delete personal information you know to have come from the child-directed site.

L. REQUIREMENT TO LIMIT INFORMATION COLLECTION

1. If I operate a social networking service and a parent revokes her consent to my maintaining personal information collected from the child, can I deny that child access to my service?

Yes. If a parent revokes consent and directs you to delete the personal information you had collected from the child, you may terminate the child's use of your service. *See* 16 C.F.R. § 312.6(c).

2. I know that the Rule says I cannot condition a child's participation in a game or prize offering on the child's disclosing more information than is reasonably necessary to participate in those activities. Does this limitation apply to other online activities?

Yes. The applicable Rule provision is not limited to games or prize offerings, but includes "another activity." *See* 16 C.F.R. § 312.7. This means that you must carefully examine the information you intend to collect in connection with every activity you offer in order to ensure that you are only collecting information that is reasonably necessary to participate in that activity. This guidance is in keeping with the Commission's general guidance on data minimization.

M. COPPA AND SCHOOLS

1. Can an educational institution consent to a website or app's collection, use or disclosure of personal information from students?

Yes. Many school districts contract with third-party website operators to offer online programs solely for the benefit of their students and for the school system – for example, homework help lines, individualized education modules, online research and organizational tools, or web-based testing services. In these cases, the schools may act as the parent's agent and can consent to the collection of kids' information on the parent's behalf. However, the school's ability to consent for the parent is limited to the educational context – where an operator collects personal information from students for the use and benefit of the school, and for no other commercial purpose. Whether the website or app can rely on the school to provide consent is addressed in FAQ M.2. FAQ M.5 provides examples of other "commercial purposes."

In order for the operator to get consent from the school, the operator must provide the school with all the notices required under COPPA. In addition, the operator, upon request from the school, must provide the school a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information. As long as the operator limits use of the child's information to the educational context authorized by the school, the operator can presume that the school's authorization is based on the school's having obtained the parent's consent. However, as a best practice, schools should consider making such notices available to parents, and consider the feasibility of allowing parents to review the personal information collected. See FAQ M.4. Schools also should ensure operators to delete children's personal information once the information is no longer needed for its educational purpose.

In addition, the school must consider its obligations under the Family Educational Rights and Privacy Act (FERPA), which gives parents certain rights with respect to their children's education records. FERPA is administered by the U.S. Department of Education. For general information on FERPA, see http://ptac.ed.gov/. Schools also must comply with the Protection of Pupil Rights Amendment (PPRA), which also is administered by the Department of Education. *See* http://ptac.ed.gov/. (*See* FAQ M.5 for more information on the PPRA.)

Student data may be protected under state law, too. For example, California's Student Online Personal Information Protection Act, among other things, places restrictions on the use of K-12 students' information for targeted advertising, profiling, or onward disclosure. States such as Oklahoma, Idaho, and Arizona require educators to include express provisions in contracts with private vendors to safeguard privacy and security or to prohibit secondary uses of student data without parental consent.

2. Under what circumstances can an operator of a website or online service rely upon an educational institution to provide consent?

Where a school has contracted with an operator to collect personal information from students for the use and benefit of the school, and for no other commercial purpose, the operator is not required to obtain consent directly from parents, and can presume that the school's authorization for the collection of students' personal information is based upon the school having obtained the parents' consent. However, the operator must provide the school with full notice of its collection, use, and disclosure practices, so that the school may make an informed decision.

If, however, an operator intends to use or disclose children's personal information for its own commercial purposes in addition to the provision of services to the school, it will need to obtain parental consent. Operators may not use the personal information collected from children based on a school's consent for another commercial purpose because the scope of the school's authority to act on behalf of the parent is limited to the school context.

Where an operator gets consent from the school rather than the parent, the operator's method must be reasonably calculated, in light of available technology, to ensure that a school is actually providing consent, and not a child pretending to be a teacher, for example.

3. Who should provide consent – an individual teacher, the school administration, or the school district?

As a best practice, we recommend that schools or school districts decide whether a particular site's or service's information practices are appropriate, rather than delegating that decision to the teacher. Many schools have a process for assessing sites' and services' practices so that this task does not fall on individual teachers' shoulders.

4. When the school gives consent, what are the school's obligations regarding notifying the parent?

As a best practice, the school should consider providing parents with a notice of the websites and online services whose collection it has consented to on behalf of the parent. Schools can identify, for example, sites and services that have been approved for use district-wide or for the particular school.

In addition, the school may want to make the operators' direct notices regarding their information practices available to interested parents. Many school systems have implemented Acceptable Use Policies for Internet use (AUPs) to educate parents and students about in-school Internet use. The school could maintain this information on a website or provide a link to the information at the beginning of the school year.

5. What information should a school seek from an operator before entering into an arrangement that permits the collection, use, or

disclosure of personal information from students?

In deciding whether to use online technologies with students, a school should be careful to understand how an operator will collect, use, and disclose personal information from its students. Among the questions that a school should ask potential operators are:

> What types of personal information will the operator collect from students?
>
> How does the operator use this personal information?
>
> Does the operator use or share the information for commercial purposes not related to the provision of the online services requested by the school? For instance, does it use the students' personal information in connection with online behavioral advertising, or building user profiles for commercial purposes not related to the provision of the online service? If so, the school cannot consent on behalf of the parent.
>
> Does the operator enable the school to review and have deleted the personal information collected from their students? If not, the school cannot consent on behalf of the parent.
>
> What measures does the operator take to protect the security, confidentiality, and integrity of the personal information that it collects?
>
> What are the operator's data retention and deletion policies for children's personal information?

Schools also should keep in mind that under the Protection of Pupil Rights Amendment, Local Educational Agencies (LEAs) must adopt policies and must provide direct notification to parents at least annually regarding the specific or approximate dates of, and the rights of parents to opt their children out of participation in, activities involving the collection, disclosure, or use of personal information collected from students for the purpose of marketing or selling that information (or otherwise providing the information to others for that purpose).

N. COPPA SAFE HARBOR PROGRAMS

1. How can I qualify as a Commission-approved COPPA safe harbor program?

To be considered for COPPA safe harbor status, an industry group or other person must submit its self-regulatory guidelines to the FTC for approval. The Rule requires the Commission to publish the safe harbor application in the Federal Register seeking public comment. The Commission then is required to make a written determination on the application within 180 days after its filing.

COPPA safe harbor applications must contain:

> A detailed explanation of the applicant's business model and technological capabilities and mechanisms it will use to assess member operator's information collection practices;
>
> A copy of the full text of the safe harbor program's guidelines and any accompanying commentary;
>
> A comparison of each program guideline with each corresponding Rule provision and a statement of how each guideline meets the Rule's requirements; and
>
> A statement of how the assessment mechanisms and disciplinary consequences provide effective COPPA enforcement.

The amended Rule sets forth the key criteria the FTC will consider in reviewing a safe harbor application:

Whether the applicant's program includes guidelines that provide substantially the same or greater protection than the standards set forth in the COPPA Rule;

Whether the program includes an effective, mandatory mechanism to independently assess member operators' compliance with the program's guidelines, which at a minimum must include a comprehensive annual review by the safe harbor program of each member operator;

Whether the program includes effective disciplinary actions for member operators who do not comply with the safe harbor program guidelines.

See 16 C.F.R. § 312.11.

2. What should I do if I am interested in submitting my self-regulatory program to the FTC for approval under the safe harbor provision?

Information about applying for FTC approval of a safe harbor program is provided in Section 312.11 of the Rule and online at the COPPA Safe Harbor Program portion of the FTC's Business Center website. In addition, you may send an email to CoppaHotLine@ftc.gov, and a member of the FTC staff will help answer your questions.

3. How can I learn about safe harbor programs that have been approved by the Commission?

Information about the applicants who have sought safe harbor status can be found online at the COPPA Safe Harbor Program portion of the FTC's Business Center website. The site includes each organization's applications and guidelines, along with comments submitted by the public, and the basis for the Commission's written determination of each application.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

March 2015