EXHIBIT I

Federal Trade Commission
Protecting America's Consumers

Frequently Asked Questions about the Children's Online Privacy Protection Rule

(Revised October 7, 2008 (updating FAQs 44 and 45))

The following FAQs are intended to supplement the compliance materials available on the FTC website. To view the Rule and compliance materials, go to the FTC website at www.ftc.gov/privacy/privacyinitiatives/childrens.html.

INDEX OF HEADINGS

GENERAL QUESTIONS

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

Congress enacted the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-6508, in 1998. COPPA contains a requirement that the Federal Trade Commission (FTC or Commission) issue and enforce a rule concerning children's online privacy, which the Commission did in 1999. The Children's Online Privacy Protection Rule, 16 C.F.R. Part 312, became effective on April 21, 2000.

The primary goal of COPPA and the Rule 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 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.
Operators covered by the Rule must:

1. Post a clear and comprehensive privacy policy on their website describing their information practices for children's personal information;
2. Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information 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;
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.

In addition, the Rule prohibits operators from conditioning a child's participation in an online activity on the child's providing more information than is reasonably necessary to participate in that activity.

2. Where can I find information about COPPA?

The FTC has a comprehensive website, http://www.ftc.gov/, that provides information to the public concerning all of the agency's activities. Clicking on the "Consumer Protection" button on the FTC's home page will take you to a welcoming page containing a prominent link entitled "Privacy Initiatives." Clicking on that will take you to the Children's Privacy section, which also is accessible by cutting and pasting the following link into a web browser: www.ftc.gov/privacy/privacyinitiatives/childrens.html. The Children's Privacy section includes a variety of materials regarding COPPA and the Rule, 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 Commission- approved COPPA safe harbor programs; FTC cases brought to enforce COPPA and the Rule; and announcements of future activities.

Hard copies of all educational materials on the FTC website also are available free of charge by calling the FTC Consumer Response Center's toll free number at (877) FTC-HELP.

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

The first thing you should do is read the staff's guidance materials, available either on the FTC website at www.ftc.gov/privacy/privacyinitiatives/childrens.html or by calling our toll free telephone number, (877) FTC-HELP. If, after reviewing the FTC's online materials, website operators or their attorneys continue to have specific COPPA compliance questions, they should call the FTC's COPPA Hotline at (202) 326-3140.

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

You may call our toll free telephone number, (877) FTC-HELP, to submit your complaint to a live operator. The FTC website also has an online form to file complaints or request information, accessible through the "File a Complaint" link at the top of the website's homepage, http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.

5. 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 Rule sets out a number of factors for determining whether a website is directed to children, such as whether its subject matter and language are child-oriented, whether it uses animated characters, or whether advertising appearing on the website is directed to children. The Commission will also consider empirical evidence regarding the actual and intended ages of the website's visitors. *See* 16 C.F.R. § 312.2 (definition of "website or online service directed to children") and the Rule's Statement of Basis and Purpose, 64 Fed. Reg. 59888 et seq., available at http://www.ftc.gov/privacy/privacyinitiatives/childrens.html, p. 59893.

6. What types of online transmissions does COPPA apply to?

COPPA applies to personal information collected online by websites and online services located on the Internet. The Rule defines "Internet" to mean the myriad of computer and telecommunications facilities that make up the world-wide networks that employ the Transmission Control Protocol/Internet Protocol (TCP/IP), or any predecessor or successor protocols used to communicate information of all kinds by wire, radio, or

other methods of transmission. See 16 C.F.R. § 312.2 (definition of "Internet"). The Rule's Statement of Basis and Purpose makes clear that the term Internet is intended to apply to broadband networks, as well as to intranets maintained by online services that either are accessible via the Internet, or that have gateways to the Internet. *See* Statement of Basis and Purpose, 64 Fed. Reg. 59888 et seq., available at http://www.ftc.gov/privacy/privacyinitiatives/childrens.html, p. 59891.

7. Does COPPA apply to information about children collected from parents or other adults?

No. COPPA and the Rule only apply to personal information collected from children, including personal information about their parents, friends, or other persons.

The Rule's Statement of Basis and Purpose, however, 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*, et seq., available at* http://www.ftc.gov/privacy/privacyinitiatives/childrens.html, p. 59902, n. 213.

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

In enacting the statute, Congress determined to apply COPPA's protections only to children under 13. Congress and industry self-regulatory bodies have traditionally distinguished children aged 12 and under, who are particularly vulnerable to overreaching by marketers, from children over the age of 12, for whom strong, but more flexible protections may be appropriate. In addition, distinguishing adolescents from younger children may be warranted where younger children may not understand the safety and privacy issues created by the online collection of personal information.

Given the risks inherent in the disclosure of personal information for all ages, the FTC encourages website operators to offer teenagers privacy protections as well. Moreover, websites' information practices regarding teens and adults are subject to Section 5 of the FTC Act, which prohibits unfair or deceptive acts and practices. See Staff Opinion Letter to Center for Media Education (July 15, 1997) for guidance on how Section 5 applies to information practices involving teens. In addition, recent concern about the risks of child participation on social networking websites led the FTC to issue a set of safety tips for social networking. *See* "Social Networking Sites: A Parents' Guide" (September 2007), *available at* http://www.ftc.gov/privacy/privacyinitiatives/childrens.html; *see also* http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.

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

Yes. The Rule governs any collection of personal information from children, even if children volunteer that information and are not required to input that information to participate on your website.

10. Hasn't COPPA been declared unconstitutional?

No. COPPA went into effect on April 21, 2000 and has never been challenged. The Child Online Protection Act (COPA), enacted on October 23, 1998, is often confused with COPPA. COPA sought to prohibit online sites from knowingly making available to minors material that is "harmful to minors." Enforcement of this law was immediately subject to legal challenge under the First Amendment. In June 2004, the Supreme Court upheld a lower court injunction against the law, ruling that it was most likely unconstitutional. The Court, however, sent the case back to the trial court to determine whether, given technological developments,

COPA is the least restrictive alternative available to accomplish Congress' goal in enacting the statute. After a trial on the merits of the case, in March of 2007, the trial court again found that COPA was unconstitutional.

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

No. COPPA is meant to give parents control over the collection, use, or disclosure of personal information from children, not the dissemination of information to children.

If you are concerned about your children accessing pornography or other inappropriate materials on the Internet, you may want to look for 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, *e.g.,* at websites such as http://www.ftc.gov/privacy/privacyinitiatives/childrens.html and http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.

COPPA ENFORCEMENT

12. How does the FTC enforce the Rule?

The FTC monitors the Internet for compliance with the Rule and brings law enforcement actions when appropriate to deter violations. Parents and others may submit complaints to the FTC through the FTC website, http://www.ftc.gov/privacy/privacyinitiatives/childrens.html, and toll free number, (877) FTC-HELP. Consumer groups, industry members, Commission-approved COPPA safe harbor programs, and other members of the public also may provide information concerning website operators that may not be in compliance with the Rule.

13. What are the penalties for violating the Rule?

A court can hold website operators who violate the Rule liable for civil penalties of up to $11,000 per violation. The amount of penalties the court assesses may turn on a number of factors, including the egregiousness of the violation, 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.

14. Do the states or other government agencies have jurisdiction over this issue?

Yes. COPPA gives states and certain federal agencies authority to enforce compliance with the Act itself (not the Rule) with respect to entities over which they have jurisdiction. For example, the Office of the Comptroller of the Currency handles compliance by national banks and the Department of Transportation handles air carriers.

15. Has the FTC sued anybody for violating COPPA?

Yes. The FTC has obtained numerous federal district court settlements against website operators who are alleged to have violated the COPPA Rule. Press releases, and the complaints and orders may be found at http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.

16. What should I do if my website isn't in compliance with the Rule?

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

Second, carefully review your information practices and 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; whether you have adequate mechanisms for providing parents with notice and obtaining verifiable consent; and whether you have adequate methods for parents to review and delete their children's information.

Educational materials aimed at website operators and others are available on the FTC's website at http://www.ftc.gov/privacy/privacyinitiatives/childrens.html. These materials can provide you with helpful guidance.

17. Are websites operated by nonprofit entities subject to the Rule?

COPPA and the Rule expressly state that they apply to commercial websites and not to nonprofit entities that would otherwise be exempt from coverage under Section 5 of the FTC Act. In general, therefore, most nonprofit 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 and the Rule, the FTC encourages them to post privacy policies on their websites and provide COPPA protections to their child visitors.

18. Does COPPA apply to websites operated by the Federal Government?

As a matter of federal policy, all websites operated by the Federal Government and contractors operating on behalf of federal agencies must comply with the standards set forth in COPPA. *See* http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.

19. The Internet is a global medium. Do websites set up and run abroad have to comply with the Rule?

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

PRIVACY POLICIES AND DIRECT NOTICES TO PARENTS

20. My site does not collect any personal information. Do I still need to post a privacy policy?

COPPA and the Rule apply only to those websites that collect or disclose personal information from children. However, the FTC recommends that all websites post privacy policies so visitors can easily learn about the website operator's information practices. Some surveys show that parents are uncomfortable with their children giving out any personal information online, so they may be pleased to read your privacy policy and discover that you do not collect personally identifiable information.

21. What information must I include in my privacy policy?

Section 312.4(b) of the Rule identifies the information that must be disclosed in your online privacy policy. Required information includes: the name, address, telephone number, and email address of each operator collecting or maintaining personal information from children through your site; the types of personal information collected from children and whether it is collected actively or passively; how such personal

information is or may be used; whether such personal information is disclosed to third parties, various other types of information about those third parties as set forth in the Rule, and that the parent may deny consent to this disclosure; that the operator cannot condition a child's participation in an activity on the disclosure of more information than is reasonably necessary to participate; and that the parent can review the child's personal information and refuse to permit the further collection or use of the child's information. 16 C.F.R. § 312.4(b)(2).

The Rule also requires that a link to the privacy policy be posted clearly and prominently on your home page and at each area where personal information is collected. 16 C.F.R. § 312.4(b).

22. Do I have to disclose in my privacy policy and direct notice my use of "cookies," "GUIDs," "IP addresses," or other passive information collection technologies?

Yes, if you intend to combine the passively collected non-personal information with "personal information." The Rule defines "personal information" to include individually identifiable information about an individual collected online, including any persistent identifier that is tied to such identifying information. Where, for instance, you maintain a persistent identifier that is tied to a child's personally identifiable information, it can be used to identify, contact, or locate an individual and thus is considered "personal information" under the Rule. *See* 16 C.F.R. § 312.2.

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

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

24. I operate a general audience website that contains a specific children's section. May I post a single privacy policy for the whole site that contains information about my children's information practices and general information practices together, or do I have to have a separate privacy policy for children's information practices?

In the Rule's Statement of Basis and Purpose, the Commission noted that "[o]perators 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 statement that there is a specific section discussing the operator's information practices with respect to children." *See* 64 Fed. Reg. 59888 *et seq., available at* http://www.ftc.gov/privacy/privacyinitiatives/childrens.html, p. 59894, n.98. In addition, the link for the children's portion of the privacy policy must appear on the home page of the children's area and at each area where personal information is collected from children.

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

It depends. The Rule requires that the link to your privacy policy "be placed in a clear and prominent place and manner on the home page of the website or online service," and at each area where children provide, or are asked to provide, personal information. *See* 16 C.F.R. § 312.4(b)(1)(ii) and (iii). In explaining this requirement, the Commission noted 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 page, or a link that is indistinguishable from a number of other adjacent links." 64 Fed. Reg. 59888 *et seq., available at* http://www.ftc.gov/privacy/privacyinitiatives/childrens.html, p. 59894. A link that is at the bottom of the page may be acceptable if the manner in which it is presented nonetheless makes it clear and prominent as explained in the Rule's Statement of Basis and Purpose.

26. What information must I include in my direct notice to parents?

Section 312.4(c)(1) of the Rule identifies the information that must be disclosed in the direct notice you send to parents. First, the direct notice must inform the parent that you wish to collect personal information from the child. Second, the direct notice must contain all the same content that the Rule requires you to set forth in your online privacy policy. Finally, the direct notice also must contain additional information, depending on how you intend to use the information you collect from children. See 16 C.F.R. § 312.4(c)(1)(ii)-(iv).

27. When I send a direct notice to parents, may I simply email them a link to my privacy policy?

You may send your direct notice to parents via email, and you may include in that email a link to your privacy policy to satisfy part of the Rule's direct notice requirement. However, even where you include a link to your privacy policy in your direct notice, the direct notice must contain the following information:

1. All direct notices must state that you wish to collect personal information from the child and what types of information you wish to collect;
2. Where you are seeking verifiable consent from the parent (see § 312.5(c)(1)), the direct notice must state that the parent's consent is required for the collection, use, or disclosure of the child's personal information, and how the parent may provide consent;
3. Where your limited collection of the child's online contact information falls within the "multiple-use" exception (see § 312.5(c)(3)), your direct notice must state: that you have collected the child's online contact information; that the parent may refuse to permit further contact with the child and direct you to delete the child's information; indicate how the parent can have the child's information deleted; and indicate that if the parent fails to respond, you may use the child's online contact information for the purpose stated in your direct notice.
4. Where your limited collection of a child's name and online contact information falls within the "child safety" exception (see § 312.5(c)(4)), your direct notice must state that the operator has collected the child's name and online contact information to protect the safety of the child, that the parent may refuse to permit the use of the information and require its deletion, and that if the parent fails to respond, the operator may use the information for the purpose stated in your direct notice.

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

Under the Rule, if there are multiple operators collecting information through your site, 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 uses of children's information, as long as the names of all the operators are also listed in the notice. *See* 16 C.F.R. § 312.4(b)(2)(i).

If you wish to keep your privacy policy and notice simple, you may include a clear and prominent link in the privacy policy or direct notice to the complete list of operators. You must ensure, however, that the privacy policy and direct notice enable parents to easily access this list.

VERIFIABLE PARENTAL CONSENT

29. 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 "email exceptions" for the collection of online contact information described in Question 30 below. *See* 16 C.F.R. § 312.5(a) and ©).

30.May I collect the information from the child first and then get consent from the parent if I don't use the information until I get consent?

In most cases, COPPA and the Rule require operators to get verifiable parental consent before collecting personal information from children under 13.

Certain, limited exceptions, sometimes referred to as the Rule's "email exceptions," let operators collect a child's, and sometimes a parent's, online contact information before obtaining parental consent. 16 C.F.R. § 312.5©). These exceptions include:

1. collecting the name or online contact information of a parent or child for the sole purpose of providing direct notice and obtaining parental consent. If consent has not been obtained after a reasonable time from the date the child's information was collected, the website operator must delete the child's personal information from its records;
2. collecting a child's online contact information solely to respond once to a specific request from the child, as long as the information provided by the child is not used to re-contact the child and is deleted immediately after responding to the child's specific request;
3. collecting a child's and a parent's online contact information in order to send the child periodic communications, such as online newsletters, site updates, or password reminders. Under this exception, immediately after the initial response to the child and before making any additional response to the child, the operator must make reasonable efforts to ensure that the parent receives notice and is informed of the opportunity to opt-out of further use of the information collected. Under this limited exception, the operator is not required to obtain the parent's affirmative consent, and the parent must contact the operator to discontinue repeated communications. Note that a website operator will not have satisfied the "reasonable efforts" requirement where he receives notification that the email sent to the parent has bounced back or delivery failed in some other manner. Information on what must be included in the parental notice is described in Question 27, above.
4. collecting a child's name and online contact information where necessary to protect the safety of a child participating on the site. Under this limited exception, the operator must use reasonable efforts to provide a parent with notice as described in Question 27 above. Note that a website operator who collects a child's name and online contact information under this "child safety" exception may only use the child's information for the sole purpose of protecting the child's safety, may not use the information to re-contact the child or for any other purpose, and may not disclose the child's information on its website or online service.
5. collecting a child's name and online contact information for the sole purpose of protecting the security or integrity of the site, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or for an investigation on a matter related to public safety.

The requirements for using each of these exceptions are set forth in Section 312.5©) of the Rule.

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

Yes, unless the information collection fits within one of the Rule's limited "email exceptions" discussed in Question 30, above. If you only use the information internally, and do not disclose it to third parties or make it publicly available, for example, through such online services as social networking sites, blogs, personal home pages, chat rooms, message boards, pen pal services, or email accounts, then you may obtain parental consent through use of the Rule's "email plus" mechanism. *See* 16 C.F.R. § 312.5(b)(2), and Question 32, below.

32. How do I get parental consent?

You can 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, in fact, the child's parent. The Rule sets forth several options:

If you are going to disclose children's personal information to third parties, or make it publicly available through operation of an online service such as a social networking site, a blog hosting service, personal home pages, chat rooms, message boards, pen pal services, or email accounts, then you must use one of the more reliable methods to obtain verifiable parental consent enumerated in the Rule:

- Provide a form for the parent to print, fill out, sign, and mail or fax back to you (the "print-and-send" method);
- Require the parent to use a credit card in connection with a transaction (which could consist of a membership or subscription fee, a purchase, or a charge to cover the cost of processing the credit card). For more on credit card transactions, see Question 33, below;
- Maintain a toll-free telephone number staffed by trained personnel for parents to call in their consent; or
- Obtain consent through an email from the parent, if that email contains a digital signature, or other digital certificate that uses public key technology obtained through one of the above methods.

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" mechanism. The "email plus" mechanism allows you to request (in the direct notice to the parent) that the parent provide consent in an email message. However, this mechanism requires that you take an additional step after receiving the parent's email consent to confirm that it was, in fact, the parent who provided consent (the "plus" factor). These additional steps include:

- Requesting in your initial email seeking consent that the parent include a phone or fax number or mailing address in the reply email, so that you can follow up to confirm consent via telephone, fax, or postal mail; or
- After a reasonable time delay, sending another email to the parent to confirm consent. In this confirmatory email, 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 revoke the consent.

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

No. First, the credit card must be verified as a real credit card by the card issuer. Most credit card companies have indicated that they do not approve of using credit card numbers without a transaction, and some say they will not verify numbers absent a transaction. Second, the transaction record provides additional assurance that the person providing consent is, in fact, the child's parent, because, through receipt of a monthly statement, the parent is given additional notice that the transaction occurred and has an opportunity to investigate any suspicious activity and revoke consent. For additional information about using a credit card to obtain parental consent, *see* 71 Fed. Reg. 13247 (Mar. 15, 2006), *available at* http://www.ftc.gov/privacy/privacyinitiatives/childrens.html, pp. 28-30.

34. Am I required to obtain verifiable parental consent if I collect the personal information through software that is downloaded from my website or from a CD-ROM that I distribute at retail outlets?

Regardless of how you initiate it, if the actual collection of personal information from children is conducted over the Internet, it is subject to the requirements of COPPA and the Rule. For example, if you invite children on your site to download software or software programs that track their online activities and then send personal information, as defined by the Rule, back to you over the Internet, then such collection would require verifiable parental consent. If the information collection does not take place via the Internet, but rather, is conducted offline, it is not subject to COPPA or the Rule.

35. What do I do if some parents cannot or will not use the consent method I've chosen? For instance, some parents may not have a credit card, or may feel uncomfortable providing credit card information over the Internet.

We recommend that you have a readily available backup method of providing consent for those parents who cannot, or will not, use your primary consent mechanism. One practical backup method to use is the print-and-send form. This method makes it easy for parents without access to email or a credit card to provide consent.

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

Giving out passwords or PIN numbers to parents is a good way to confirm a parent's identity for future contacts. Remember that if, after obtaining consent from a parent, you change your information practices in a material way, you will have to send a new notice to the parent and obtain consent to the new practices. If you have given the parent a password or a PIN number in your initial consent process, then obtaining new consent from the parent may be easier.

In addition, COPPA and the Rule require you to give parents access to any information you have collected from their children. Before you give out that information, you will need to confirm that the person requesting the information is, in fact, the child's parent. Again, giving the parent a password or PIN number during the initial consent process makes it easier to confirm the identity of that parent if access to the child's information is later requested.

37. 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?

By the Rule's own terms, you must give parents a choice about consenting to the internal collection of a child's personal information, or to the disclosure of such information, only where the disclosure of the information is not inherent in the activity to which the parent is consenting. [Note that the Rule's definition of "disclosure" is broader than merely releasing the information to third parties, and also includes "making the information publicly available in identifiable form, by any means, including by a public posting through the Internet, or through a personal home page posted on a website or online service; a pen pal service; an electronic mail service; a message board; or a chat room." 16 C.F.R. § 312.2.] In the case of social networking sites, chat rooms, message boards and other similar online services, sharing of personal information is part of the nature of the site. Therefore, 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, where the public disclosure of information is integral to the website's operations. You must, however, clearly disclose the websites' information collection and disclosure practices in your privacy oftlinepolicy and direct notice to parents so that parents can make an informed decision.

GENERAL AUDIENCE AND TEEN SITES

38. I have a website that is intended for teenagers. How does COPPA affect me?

Although you may intend for your site to target only teenagers, your site still may attract a substantial number of children under 13. A teen-directed site can identify which visitors are under 13, for example, by asking age when visitors are invited to provide personal information. For sites that choose to age-screen, age information should be asked in a way that does not invite falsification. *See* Question 39, below. In addition, we recommend that sites that choose to age-screen employ temporary or permanent cookies to prevent children from back-buttoning to change their age in order to circumvent the parental consent requirement or obtain access to the site.
Once you identify those children under age 13, you have a number of options:

1. You can collect their parents' email addresses to provide direct notice and implement COPPA's parental consent requirements; or,
2. If you do not wish to implement the COPPA protections for visitors under age 13, you could configure your data system to automatically delete the personal information of those visitors under 13 and direct them to content, if available, that does not involve collection or disclosure of personal information.

You should also consider whether you fall into one of the exceptions to the requirement of prior parental consent. For example, if you are only collecting an email address, you may be covered by one of the email exceptions described in Question 30, above.
Many sites have found creative ways to provide rich content for children, while complying with COPPA. For example, sites may choose to:

- Offer activities that do not require the collection or disclosure of personal information;
- Use screen names or other anonymous techniques to personalize the site;
- Use the email exceptions to prior parental consent; or
- Limit the amount of personal information collected and obtain prior parental consent.

39. Can I block children under 13 from my general audience website?

Blocking children under 13 from participating in a general audience, or teen-directed, website does not violate COPPA. However, as described in Question 38, above, should you choose to block children under 13, it is important that you design your age collection input screens in a manner that does not encourage children to provide a false age in order to gain access to your site. If you take reasonable measures to screen for age, then you are not responsible if a child misstates his or her age. For example:

- Ask age information in a neutral manner at the point where you invite visitors to provide personal information or to create their log-in user ID. In designing a neutral age-screening mechanism, you might 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 to freely 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 age on that site.
  - Not encouraging children to falsify their age information, for example, by stating that visitors under 13 cannot participate on your website or should ask their parents before

participating. In addition, a site that does not ask for neutral date of birth information but rather simply includes a check box stating “I am over 12 years old” would not be considered a neutral age-screening mechanism.

- In addition, we recommend using a temporary or a permanent cookie to prevent children from back-buttoning to enter a different age.

Note, however, that if you ask participants to enter age information, and then you fail to either screen out or obtain parental consent from those participants who indicate that they are under 13, you may be liable for violating COPPA and the Rule.

40. I operate a general audience site and do not ask visitors to reveal their ages. I do have a button that users can click to send feedback, comments, or questions by email. What are my responsibilities if I get an email that says, “Hi, I am Steve, age 10, and I really like your site. When do you think you will add some more games?”

Under the Rule’s one-time contact exception, 16 C.F.R. § 312.5(c)(2), you may reply to the child once without sending notice to the parent or obtaining parental consent, if you do not re-contact the child, and you delete the child’s personal information, including email address, from your records after responding to the email.

41. I operate a general audience site and do not ask visitors to reveal their ages. However, I do permit users to create their own blog pages, and my site has a number of chat rooms.

(a) What happens if a child registers on my site and posts personal information on his blog page or in a chat room, but nowhere does he reveal his age?

The Rule is not triggered. The Rule applies to operators of general audience websites if they have actual knowledge that a particular visitor is a child. If a site knows that a particular visitor is a child, then the Rule must be followed with respect to that child. *See, e.g.*, U.S. v. Xanga.com, Inc., Civil Action No. 06-CIV-6853 (SHS) (S.D.N.Y., entered Sept. 12, 2006), available at http://www.ftc.gov/privacy/privacyinitiatives/childrens.html. If a child posts personal information on a general audience site but doesn’t reveal his or her age, and you have no other information that would lead you to know that the visitor is a child, then you would not have “actual knowledge” under the Rule and would not be subject to its requirements. Note, however, that even where a child himself has not revealed his age on the site, actual knowledge will be present where a site learns of a child’s age, for instance, from a concerned parent who has discovered that his child is participating on the site. *See* Rule’s Statement of Basis and Purpose, 64 Fed. Reg. 59888 et seq., *available at* http://www.ftc.gov/privacy/privacyinitiatives/childrens.html, p. 59892.

(b) What happens if a child visits a chat room or creates a blog and announces his or her age?

You may be considered to have actual knowledge with respect to that child if someone from your organization sees the post, or if someone alerts you to the post (for example, a concerned parent who learns that his child is participating on your site). However, if no one in your organization is aware of the post, then you may not have the requisite actual knowledge under the Rule.

If you have monitored chat rooms where monitors delete information from posts before they are made public, then your monitors can simply strip the child’s posts of any personal information before they are

publicly posted, thus permitting children to participate in the chat room without the need for obtaining parental consent. This practice is easily applied to “auditorium” style chat rooms in which children pose questions that a moderator screens before posting, and may work well for other websites with chat features.

EXCEPTIONS TO PRIOR PARENTAL CONSENT

42. I want to have a contest on my site. Can I use the one-time contact exception to prior parental consent?

Yes, if you collect children’s email addresses, and email addresses only, 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 email addresses.

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 email address 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 email addresses 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 an email address in connection with contest entries – such as collecting a winner’s home address to mail a prize – you must provide parents with direct notice and affirmatively obtain prior parental consent, as you would for other types of personal information collection beyond an email address. 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 email address so that the parent may be notified if the child wins the contest. In the prize notification email, you can ask the parent to provide the home mailing address to ship the prize, or invite the parent to call a telephone number to provide the mailing information.

43. I have a site 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?

No. This feature will likely fall under the one-time contact exception. If your site simply answers the child’s question and then deletes the child’s email address (and does not otherwise maintain or store the child’s personal information in any form), you fall into the one-time contact exception and do not need to obtain parental consent.

44. My child-directed website wants to offer electronic post cards and the ability for children to forward items of interest on my site to their friends. Can I take advantage of one of the email exceptions to parental consent?

It depends on how you design your e-card or forward-to-a-friend system. Any system providing the opportunity to reveal any personally identifiable information (PII) other than the recipient’s email address requires you to obtain heightened verifiable consent from the sender’s parent, and does not fall within one of COPPA’s limited exceptions. This means that if your e-card/forward-to-a-friend system permits PII to be disclosed in either the “from” or “subject” lines, or in the body of the message, then you must notify the sender’s parent and obtain parental consent using one of the more reliable methods to obtain verifiable consent enumerated in the Rule *before* collecting any PII from the child.

In order to take advantage of COPPA’s one-time contact exception for your e-cards, your webform may only ask for recipient’s email address (and, if desired, sender and/or recipient’s first name and last initial). Your e-card system must not permit the sender to enter her full name, her email address, or the recipient’s full name. In addition, you may not provide users with the ability to freely type messages in either the subject

line of the e-card or in any text fields.

Finally, you should immediately send the e-card, and then automatically delete the recipient's email address after sending. If you choose to retain the recipient's email address until some point in future (*e.g.*, until e-card is opened by the recipient, or if you allow the sender to indicate a date in the future when the e-card should be sent), you must collect the sender's parent's email address and provide notice and opt-out to sender's parent *before* the e-card is sent. *See* Statement of Basis and Purpose, 64 Fed. Reg. 59888 *et seq*., available at http://www.ftc.gov/privacy/_°_Ô, p. 59902, n.222.

45. 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 the email address for users who are under age 13?

If you plan to retain the child's email address in retrievable form after the initial collection, to be used, for example, to directly email children reminders of their passwords, then you must provide notice to parents and the opportunity to opt-out under the "multiple-contact" exception. *See* §312.5(c)(3) and FAQ 42 above.

However, where no other personally identifying information is collected from children or can be disclosed on your website by children themselves, you may collect email addresses from children without first providing notice to parents and giving them the opportunity to opt-out if you immediately alter the email addresses (*e.g.*, through "hashing") such that they can no longer be reconstructed into their original form but the hashed form can be used to create a password reminder system. If you collect and immediately hash email addresses without notifying parents, you should clearly and conspicuously explain this process both at the point of collection and in your site's privacy policy, so that your users are aware of how their 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 notice.

PARENTAL ACCESS

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

No. As the Commission noted in the Rule's 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 Rule's Statement of Basis and Purpose, " 64 Fed. Reg. 59888, et seq., available at www.ftc.gov/os/1999/10/64fr59888.pdf, p. 59904.

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

Reasonable methods for verifying that a person seeking access to a child's information is the parent, taking into account available technology, include: providing a mailing address or fax number for the parent to make the request in writing; providing a toll-free number staffed by trained personnel for a parent to call; using a credit card in connection with a transaction; using digital signatures; using an email accompanied by a PIN or password obtained through one of the above methods; or submission of a driver's license. See Statement of Basis and Purpose, " 64 Fed. Reg. 59888, et seq., available at www.ftc.gov/os/1999/10/64fr59888.pdf, p. 59905. Under the Rule, if you act in good faith and follow reasonable procedures to verify that the requestor is the parent, then 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(b).

DISCLOSURE OF INFORMATION TO THIRD PARTIES

48. If I want to share information collected from children with a corporate affiliate, how does the Rule apply?

The answer depends on the affiliate's relationship to and use of the personal information you have collected from children. If you disclose children's personal information to an affiliate solely for it to provide internal support for you or your website, and you require the affiliate to keep the information confidential and use it for no other purpose, then the use is internal and the affiliate is not considered to be a third-party operator under the Rule. Similarly, an affiliate is not an operator under the Rule if it plays no role in collecting, maintaining, or using personal information from children.

If you plan to share children's personal information with an affiliate for any reason other than providing internal support for you or your website, such as for its own marketing campaign, the Rule requires you to notify parents (in your privacy policy and direct notice) that you want to disclose their children's personal information to an affiliate. As part of this notice, you must state whether the affiliate has agreed to be bound by your privacy policy. You also must give parents an opportunity to opt out of the disclosure to the affiliate as part of the consent process.

REQUIREMENT TO LIMIT INFORMATION COLLECTION

49. I know that I cannot condition a child's participation in a game or the offering of a prize on the child giving out more information than is reasonably necessary to participate in those activities, but does that limitation apply to other online activities?

Yes. Section 312.7 of the Rule provides: "An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more information than is reasonably necessary to participate in such activity." Therefore, you must carefully examine the information you collect in connection with each activity you offer on your site to ensure that you are only collecting information that is reasonably necessary to participate in that activity.

50. If I operate a chat room and a parent revokes his or her consent to my maintaining personal information collected from the child, can I deny that child access to my chat room?

Yes. If a parent revokes consent and directs you to delete the personal information you had collected that was necessary for the activity, you may terminate the child's use of that service or the child's participation in that service. See 16 C.F.R. § 312.6©).

SAFE HARBORS

51. How can organizations with self-regulatory guidelines qualify for safe harbor treatment?

The organization must submit its guidelines to the FTC for approval. The Commission will publish submissions for public comment and then make a determination of whether the guidelines meet the criteria set forth in the Rule. The key criteria are that the guidelines provide the same or greater protections for children as the Rule; provide effective, mandatory mechanisms for assessing participants' compliance with the requirements; and offer compliance incentives that provide for effective enforcement of the Rule. See 16 C.F.R. § 312.10(b).

52. 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 312.10 of the Rule and at our website at www.ftc.gov/privacy/privacyinitiatives/childrens_shp.html. In addition, you may call the COPPA Hotline at (202) 326-3140, and a member of the FTC staff will help answer your questions.

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

Four groups have been approved as COPPA safe harbor programs so far: the Children's Advertising Review Unit of the Better Business Bureaus (CARU); the Entertainment Software Rating Board (ESRB); TRUSTe; and Privo, Inc. Their applications and final guidelines are posted on the FTC website at http://www.ftc.gov/privacy/privacyinitiatives/childrens.html, along with public comments on the applications and the basis for the Commission's decisions.

SCHOOLS AND WEB SERVICES DIRECTED TO SCHOOLS

54. Does the Rule place requirements or restrictions on schools regarding the collection or disclosure of students' personal information on the Internet?

COPPA allows, but does not require, schools to act as agents for parents in providing consent for the online collection of students' personal information within the school context. See Statement of Basis and Purpose, " 64 Fed. Reg. 59888, et seq., available at www.ftc.gov/os/1999/10/64fr59888.pdf, p. 59904. In this regard, schools also must consider their obligations under the Family Educational Rights and Privacy Act (FERPA), which is administered by the U.S. Department of Education. For general information on FERPA, see www.ed.gov/policy/gen/guid/fpco/ferpa.

Many schools have implemented Acceptable Use Policies (AUPs) or other measures to educate parents and students about in-school Internet use. For example, a school may use the AUP to inform parents of what online services are provided to students, and the school's policies regarding students' use of the Internet.

55. Does COPPA apply to website operators that contract with schools to provide online services involving the collection, use or disclosure of students' personal information?

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, e.g., homework help lines or web-based testing services. COPPA does not apply to the website operator's collection of personal information from participating children 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. Thus, 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. The operator should, however, provide the school with full notice of its collection, use, and disclosure practices, so that the school may inform parents of these practices in its Acceptable Use Policy.