



How to Comply With The Children's Online Privacy Protection Rule (COPPA) Updated Rule Released July 1, 2013

Since April of 2000, the Children's Online Privacy Protection Act (COPPA) has been in effect. The purpose of this law is to give parents greater control over what information their children can access over the Internet. In general, the law requires operators of commercial web sites and online services such as mobile apps, network-connected games, online purchasing, VOIP services, Internet-enabled gaming platforms, and location services to provide notice and obtain parent's consent before collecting personal information from children under the age of 13.

Effective July 1, 2013, the Federal Trade Commission (FTC), citing changes in technology, updated the COPPA Rule and expanded its definition of who and what is covered under COPPA. It is important to know if your company is covered under the new COPPA Rule, what you're responsibilities are and how to comply with the revised Rule.

The following are some practical definitions and core elements of the new COPPA Rule. This is not legal advice. We do recommend that you visit the [FTC website](#) and consult with legal representation to ensure full compliance.

This fact sheet covers:

- ◆ How COPPA applies to your company and what information is covered.
- ◆ What elements to include in a privacy policy statement and direct notice to parents.
- ◆ How and when to obtain parent's verifiable consent before collecting information from their kids.
- ◆ How to protect the security of kids' personal information.
- ◆ What to do about information that was collected prior to the new Rule's effective date.
- ◆ Information about COPPA Safe Harbor Programs.

A. DOES YOUR WEBSITE OR ONLINE SERVICE COLLECT PERSONAL INFORMATION FROM KIDS UNDER 13?

Who Must Comply?

- ◆ Operators of commercial web sites or online services that are “directed to children” (under 13) and collect personal information from children.
- ◆ Operators of general audience web sites or online services who have “actual knowledge” that they collect personal information from children.
- ◆ **New: Third parties (e.g., social plug-ins and ad networks) with actual knowledge that they are collecting personal information directly from users of another site or online service directed to children.**
- ◆ **First parties are strictly liable for actions of third parties on first party’s site or service.**

What Information is Covered?

Under the previous rule, certain factors were considered when deciding if information was directed to children. For instance:

- ◆ Subject matter,
- ◆ Visual content,
- ◆ Animated characters,
- ◆ Child-oriented activities and incentives,
- ◆ Age of models, and
- ◆ Ads that promote or appear on the property.

Under the revised rule, **new factors** have been added:

- ◆ **Music/audio content, and**
- ◆ **Presence of child celebrities/celebrities that appeal to children.**

Personal Information (PI):

COPPA applies to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number, Social Security Number or any other information that would allow someone to identify or contact the child. As well as other identifiable information such as hobbies, interests and information collected through cookies or other types of tracking mechanisms.

Under the revised rule, **new factors** have been added:

- ◆ **A screen or user name that functions as online contact information (includes email address, does NOT include content personalization, filtered chat, public display, operator-to-user communication, or the use of screen names to allow children to log-in across devices.)**
- ◆ **Persistent identifier that can be used to recognize a user over time and across different web sites or online services (includes IP address).**
- ◆ **Photograph, video, or audio file that contains a child’s image or voice (does not include blurred photos or cropped photos, but must also remove metadata that is personal identifiable information.)**

- ◆ **Geolocation information sufficient to identify street and city or town.**
- ◆ **NOT: Zipcode, Date of Birth or Gender.**

What is the First Party Liability?

Under the previous rule, operators may be liable for agents or service providers. The new Rule expands liability to cover third parties that collect personal information directly from users of the site or service, if the operator benefits. It is not required but it is recommended to advise third parties of this expanded definition.

There is strict liability: please investigate your company's practices and make arrangements for COPPA compliance. Violations can result in law enforcement actions, including civil penalties, so compliance is required.

This Rule is not meant for platforms that simply offer access for the public to find content provided for any another company. For example, mobile app market providers are not covered under COPPA.

What is the Third Party Liability?

What happens, if for instance, one of your employees, representatives or content providers realizes that your ads are being placed in a child-directed site? Then you have actual knowledge and you must take the following steps.

- 1) Stop collecting personal information.
- 2) Delete all the previous information or take it offline and store it pending parental consent.
- 3) If you do not get parental consent, then delete the information.

B. POST A PRIVACY POLICY THAT COMPLIES WITH COPPA. NOTIFY PARENTS DIRECTLY BEFORE COLLECTING PERSONAL INFORMATION FROM THEIR KIDS.

Notice and Consent Obligations:

Under COPPA, if personal information (PI) is collected from children then you are required to provide a direct and online notice to parents with verifiable parental consent (unless exception prevails).

What Should Be Included in Your Privacy Notice?

By streamlining the Rule's online notice requirements, the FTC hopes to encourage operators to provide clear, concise descriptions of its 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). Be sure to include:

- ◆ The operators', or designated operator's, contact information to respond to inquiries regarding collection and use of children's personal information.
- ◆ A description of what information the operator collects, including whether kids personal information is to be publicly available, the operators' use and disclosure practices of such information; and
- ◆ An explanation and process for how parents can review or delete a child's PI and refuse further collection.
- ◆ **Location of Link:** needs to be on the home page, landing page, or screen and each area where PI is collected, in close proximity to information requests.
- ◆ **For apps:** the privacy link is not required at the point of purchase, but prior to collection.

What is Direct Notice to Parents?

Previously, a link to an online notice was acceptable. Now, parents must be provided with a direct notice of the operator's personal information collection, use and disclosure practices. Certain requirements must be met depending on how and for what purpose information is collected and used:

- ◆ Generally, a parent's verifiable consent must be received prior to the collection, use, or disclosure of a child's personal information.
- ◆ You should provide means by which a parent can provide consent to the collection of PI without consenting to the disclosure of the information to third parties.
- ◆ You should state that the child has provided parent's contact information and provide name of the parent or child and reason why information was collected.
- ◆ If a parent doesn't consent, operator won't collect, use or disclose any of the children's PI.
- ◆ If a parent doesn't consent, operator must delete the parent's online contact information.
- ◆ Provide additional items of PI that you intend to collect and potentially disclose should the parent consent.
- ◆ Provide hyperlink to company's online privacy policy statement.
- ◆ **Please consult with the FTC and/or legal representation for further guidance and specific elements required in the direct notice FAQ C #11:**
<http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions> .

Consent Exceptions

The regulations include several exceptions that allow operators to collect a child's email address without getting the parent's consent in advance, but direct notice is still required to notify parents of what information has been collected and what their choices are regarding information. These exceptions cover many popular online activities for kids, including contests and online newsletters. Prior parental consent is not required:

- **To Give Notice and Obtain Consent:** Only purpose of PI collection is to provide notice and obtain parental consent.
- **Voluntary Notice:** Purpose of PI collection is to provide voluntary notice to the parent where service does not otherwise collect, use or disclose the child's PI.

- **One-Time:** Only purpose of PI collection is to respond to a one-time request from the child.
- **More Than Once:** Respond more than once directly to a child’s request and the information was not otherwise used.
- **Safety:** Purpose of PI collection is protecting the child’s safety.
- **Protections:** Purpose of PI collection is to protect the site or service, protect against liability, respond to judicial process, or to extent permitted by law.

Please Follow FTC Guidance for Neutral-Age Screening:

There is a new compliance option for sites or services that are “directed to children” but not as a primary audience. You may age screen all users and apply the notice and consent requirements only for users who identify themselves as under the age of 13.

- **Design your service in a manner that does not encourage children to falsify their ages (e.g., do not state that visitors under 13 cannot participate).**
 - **Ask age information at the point at which you invite PI collection or to create a user ID.**
 - **Make sure the data entry point allows accurate entry of age (e.g., cannot only offer ages 13 or older in a drop-down menu).**
- ◆ Keep in mind the FTC’s factors, and prepare to change things if necessary.
 - ◆ If your site is directed toward children, you cannot block them from entering your site. You may, however, differentiate between what users can do based on age.
 - ◆ If your site is directed toward teenagers, you need to think of your actual audience or likely audience, and whether it attracts a substantial number of children. If so, you may be considered “child-directed”.

C. GET PARENTS’ VERIFIABLE CONSENT BEFORE COLLECTING INFORMATION FROM THEIR KIDS.

What is Verifiable Parental Consent?

Before collecting, using or disclosing personal information from a child, an operator must obtain verifiable parental consent from the child’s parent, including material changes. The operator must give parents the option to consent to use but not disclose to third parties.

How to Obtain Parental Consent – You should make a reasonable effort to obtain a parent’s consent (*given available technology, new methods are allowed*) by:

- **scanned**, mailed, faxed signed consent form;
- credit card, **debit card, other online payment system (in connection w/ monetary transaction);**
- toll-free number;

- **video conference to trained personnel; and**
- **government-issued ID checked against database.**

You may apply to the FTC to approve new parental consent methods and an app store log-in is not considered sufficient. Additionally, parents have the right to review PI provided by their child.

“Email Plus” Consent

If you are going to use children’s personal information only for internal purposes (FTC FAQ I. #5: <http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions>) 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. Be sure to take an additional confirming step after receiving the parent’s message (this is the “plus” factor), includes:

- Requesting in your initial message to the parent, that he/she include a phone/fax number or mailing address in the reply message, for following up with a confirmation phone call, fax or letter to the parent; or
- After a reasonable period of time, sending another message via the parent’s online contact information to confirm consent. Be sure to include all the original information contained in the direct notice, inform the parent that he/she can and how to revoke the consent.

Safe Harbor Program: FTC-approved safe harbor program may approve member’s use of a different consent method, please consult with the FTC or legal representation.

D. IMPLEMENT REASONABLE PROCEDURES TO PROTECT THE SECURITY OF KIDS’ PERSONAL INFORMATION

Security: Operator must have “reasonable procedures” to protect the confidentiality, security, and integrity of PI collected from children.

Retention and Deletion: Operator may retain PI only as long as reasonably necessary, and must delete PI using reasonable measures.

E. WHAT ABOUT INFORMATION ALREADY COLLECTED?

- ◆ **Geolocation** - you must ask for parental consent immediately.
- ◆ **Photos, Videos or Audio Files** that contain a child’s image or voice – you don’t *need* consent for this but as a best practice you should discontinue the use or disclosure of these files.
- ◆ **Screen names** - also not covered unless the operator associates new information with it after July 1st.
- ◆ **Persistent Identifiers** – there are exceptions – please consult FTC FAQs or legal representation.

F. SAFE HARBOR PROGRAMS

You may apply for approval of a self-regulatory COPPA Safe Harbor Program if it:

- ◆ Provides substantially the same or greater protections for children,
- ◆ Shows mandatory means for independent assessment of operators' compliance with the program, and
- ◆ Includes disciplinary actions for non-compliance.

There will be an annual audit of members and annual reporting to the FTC which will include aggregate assessment details and any disciplinary actions.

FTC RESOURCES:

- ◆ General Information for Businesses on COPPA: <http://www.business.ftc.gov/privacy-and-security/childrens-privacy>
- ◆ 6-step plan to assist companies in complying with COPPA: <http://www.business.ftc.gov/documents/bus84-childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business>
- ◆ FAQ on COPPA: <http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions>
- ◆ Questions for FTC: CoppaHotLine@ftc.gov

DMA MEMBER QUESTIONS?

Members may email DMA at ethics@the-dma.org

© [Direct Marketing Association](http://www.directmarketing.org)