National Programs
Children's Advertising Review Unit®

BBB National Programs
Children's Advertising Review Unit
bbbprograms.org/CARU

Self-Regulatory Guidelines for Children's Online Privacy Protection

Table of Contents

1. What Changed with COPPA (2025)

The updated Guidelines incorporate the 2025 amendments to the Children's Online Privacy Protection Rule. Key updates include:

1. Expanded definitions of personal information (biometric identifiers, government-issued IDs);
2. Defines mixed audience website or online service as one directed to children but not targeting children as its primary audience;
3. Separate, opt-in parental consent for third-party disclosures and targeted advertising;
4. Enhanced online notice requirements (third-party categories and internal-operations purposes);
5. A published, written data retention and deletion policy;
6. Updated verifiable parental consent methods (Text-plus/SMS, knowledge-based authentication, and government-issued ID that matches an image of the parent's face);
7. A voice-files exception where audio is collected solely to respond to a child's request with prompt deletion;
8. Clarified expectations for neutral age-screening in mixed-audience services; and
9. Requires operators to maintain a written information security program that considers the risk of the type of children's personal information and the operator's activities.

2. Foundation of the Guidelines

These Guidelines address concerns about the collection of personal data from children and other privacy-related practices on the Internet. Its provisions are consistent with the Children's Online Privacy Protection Act of 1998 (COPPA) and the FTC's implementing Rule, as amended April 22, 2025 (effective June 23, 2025). These Guidelines will be interpreted in harmony with the Act and Rule. Online data collection from children poses special concerns: the medium makes it easy to collect data directly and passively from children without the supervision of parents or guardians. Young children, however, may not understand the nature of the information being sought or its intended uses, and the medium makes it easy to collect such data directly and passively from children without the supervision or permission of their parents or guardians. The collection of personal information from children,[1] as defined in Data Collection below, therefore triggers special privacy and security concerns.

The guidelines below address those concerns by providing guidance on specific issues involving online data collection and other privacy-related practices by operators of a website or other online service that 1) targets children under 13 years of age (based on the criteria set forth in the definition of website or online services directed to children in Section 312.2 of the COPPA Rule); 2) has actual knowledge that it is collecting or maintaining personal information from a child under 13 years of age; or 3) has actual knowledge that it is collecting personal information directly from users of another website or online service directed to children.[2]

3. Scope

The principles apply to online data collection and other privacy-related practices by operators that (1) target children under 13 years of age; (2) have actual knowledge that a visitor is a child under 13; or (3) have actual knowledge that they collect personal information directly from users of another child-directed website or online service. This includes mixed-audience services, which must implement neutral age-screening and prevent the collection, use, or disclosure of personal information from users who identify as under 13 unless COPPA notice and verifiable parental consent requirements are met.

1 The definitions of "collection," "operator," "parent," and "personal information" in the Children's Online Privacy Protection Rule apply whenever these terms are used in the Online Privacy Protection Guidelines. See 16 CFR § 312.2.

2 This category of companies might include operators of plug-ins or third party advertising networks who are notified by an operator of the child-directed nature of the operator's website. CARU considers these to be "Passthrough operators" since they become "operators" of a child-directed website or online service only by virtue of actual knowledge.

4. Guidelines

a. Data Collection

1. **Personal Information.** *Personal information* is defined under COPPA as individually identifiable information collected online, including: first and last name; home or physical address; online contact information such as email address, instant messaging identifier, VOIP identifier, video chat identifier, mobile phone number; a screen or user name functioning as online contact information; a phone number; a persistent identifier usable to recognize a user over time and across different websites or online services, e.g., a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or a unique device identifier; a photo, video, or audio file where such file contains a child's image or voice; geolocation information sufficient to identify street name and city or town; biometric identifiers, e.g., fingerprints, handprints, retina or iris patterns, voiceprints, gait patterns, facial templates, faceprints, or genetic data; government-issued identifiers, e.g., Social Security number, state ID, birth certificate, passport numbers; or information concerning the child or the parents of that child when combined with information contained in this definition.

2. **Disclosures and notice.** When collecting[3] information from children under 13 years of age, operators must clearly disclose their information collection and tracking practices, the purposes for which the information is used, and the means for correcting or removing information. Disclosures must be prominent and readily accessible before information is collected. Online notices must identify the identities and categories of third parties receiving children's personal information and the purposes for such disclosures. Notices must also explain that a parent may consent to collection or use of their child's personal information without consenting to third-party disclosures, unless such disclosures are integral to the service. Notices must state that, if the operator collects a persistent identifier from a child solely to provide a service, the operator limits that identifier's use to that purpose. If the operator is relying on the support for the internal operations exception to the Rule's verifiable parental consent requirement, the online notice must state the specific internal operations for which the operator has collected a persistent identifier and the means the operator uses to ensure that the identifier is not used or disclosed to contact a specific individual. If the operator is relying on the audio file exception to the Rule's verifiable parental consent requirement, the online notice must describe how the operator uses audio files containing a child's voice and state that the operator deletes such audio files immediately after responding to the request for which they were collected.[4]

3 Collects or collection means the gathering of any personal information from a child by any means, including but not limited to: (a) Requesting, prompting, or encouraging a child to submit personal information online; (b) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or (c) Passive tracking of a child online.

4 See § 312.4(d)

3. **Child-friendly explanations.** Operators should disclose, in language easily understood by a child, why the information is being collected and whether the information is intended to be shared, sold, or distributed outside of the collecting company.

4. **Passive collection.** Operators should disclose passive means of collecting information from children such as navigational tracking tools, browser files, persistent identifiers, and what information is being collected. Operators should also disclose, in general terms, the internal operations for which persistent identifiers are collected and the safeguards used to prevent misuse, such as training, data segregation, and contractual restrictions.

5. **Verifiable parental consent (VPC).** Operators must obtain VPC before collecting any personal information from children, subject to the exceptions enumerated in section 312.5(c) of the Rule and discussed in Guidelines 4.a.2 above and 10 below.[5] Where personal information will be disclosed to third parties, a separate, opt-in VPC for that disclosure, including for targeted advertising or other non-integral uses, is required. Access to the service may not be conditioned on granting that separate consent.

6. **Public posting safeguards.** For activities that involve public posting, operators should encourage children not to use their full names or screen names that correspond with their email address, but choose an alias (e.g., "Bookworm," "Skater," etc.) or use first name, nickname, initials, etc. If children do use personal information, including online contact information, in their public postings, operators must obtain parental consent.

7. **Parental review.** Operators must offer a way for parents to request access to their child's personal information and to verify that the requester is actually the child's parent. Parents must be given the ability to review what personal information has been collected from their child, to direct the operator to delete their child's information, and to revoke permission for any further collection or use of their child's information.[6]

8. **Data minimization.** Operators cannot require a child to disclose more personal information than is reasonably necessary to participate in the online activity (e.g., play a game, enter a contest, etc.).

9. **Internal operations exception for VPC for third-party disclosures.** Operators must obtain VPC before they disclose personal information to third parties.[7] However, disclosures to an entity or person that provides support for the internal operations of the operator's website or online service and who does not use or

5 See 16 CFR § 312.5.
6 See 16 CFR § 312.6.
7 Third party means any person who is not: (a) An operator with respect to the collection or maintenance of personal information on the website or online service; or (b) A person who provides support for the internal operations of the website or online service and who does not use or disclose information protected under this part for any other purpose.

disclose such information for any other purpose does not require separate VPC.[8] Information collected for internal operations must be used and disclosed only to carry out those operations and not for profiling, behavioral advertising, or amassing a profile on a specific individual.

10. **Email-plus and Text-plus VPC for Internal-use-only collection.** When an operator collects personal information only for its internal use and there is no disclosure to a third party, the operator may obtain parental consent through the use of email or text message, coupled with additional steps to provide assurance that the person providing consent is the parent. Generally, acceptable VPC methods include: email-plus (for internal use only), government ID or payment verification, phone or video confirmation, Text-plus (SMS with direct notice and consent where no third-party disclosure occurs), and knowledge-based authentication (KBA). See §312.5(b)(2).

11. **Exceptions to prior parental consent.** Prior consent is not required in the following circumstances:

    a. Collecting the parent's name or online contact information solely to provide notice and obtain parental consent.

    b. Collecting a parent's online contact information to provide voluntary notice to, and subsequently update the parent about, the child's participation in a service that does not otherwise collect, use, or disclose children's personal information.

    c. Collecting a child's online contact information solely to respond once to a specific request and then deleting it without further use or disclosure.

    d. Collecting a child's and a parent's online contact information to respond directly more than once to the child's specific request (e.g., newsletters or contests), with direct parental notice and no other use, disclosure, or combination with other data.

    e. Collecting a child's and a parent's name and online contact information to protect the safety of a child, where such information is not used or disclosed for any purpose unrelated to the child's safety.

8 Support for the internal operations of the website or online service means those activities necessary to:
(a) maintain or analyze the functioning of the website or online service;
(b) perform network communications;
(c) authenticate users of, or personalize the content on, the website or online service;
(d) serve contextual advertising on the website or online service or cap the frequency of advertising;
(e) protect the security or integrity of the user, website, or online service;
(f) ensure legal or regulatory compliance; or
(g) fulfill a request of a child as permitted by these guidelines;
so long as the information collected for the activities listed in paragraphs (a)-(g) is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose. Support for the internal operations includes, e.g.: intellectual property protection, payment and delivery functions, spam protection, optimization, statistical reporting, or de-bugging. See 78 Fed. Reg. 3981 (Jan. 17, 2013)

f. Collecting a child's name and online contact information to: (i) protect the security or integrity of the website or online service; (ii) take precautions against liability; (iii) respond to judicial process; or (iv) provide information to law enforcement or for a public safety investigation, to the extent permitted by law, and where such information is not used for any other purpose.

g. Collecting a persistent identifier and no other personal information where the identifier is used solely to provide support for the internal operations of the website or online service.

h. Where an operator covered under paragraph two (2) of the definition of website or online service directed to children collects a persistent identifier and no other personal information from a user who affirmatively interacts with the operator and whose previous registration indicates the user is not a child.[9]

i. Voice files exception: collecting audio containing a child's voice solely to respond to a child's specific request, with immediate deletion and no other personal information collection.

12. **Email communications.** If an operator communicates with a child by email, each mailing should provide an easy opportunity, such as by return email or hyperlink, for the child or parent to discontinue receiving future communications.

b. Information Security

1. **Written information security program.** Operators must designate one or more employees to maintain a written information security program that protects children's personal information considering the sensitivity of the personal information collected. The program must, among other things, be regularly tested and evaluated at least annually. Operators are also responsible for ensuring that any third parties they share children's personal information with comply with this provision (and other provisions as applicable).[10]

c. Data Retention and Deletion

1. **Use of data collected for VPC.** Operators must delete the name and contact information of a parent or child collected in order to obtain VPC if the parent does not provide consent within a reasonable time from when the notice was sent.[11]

2. **Retention policy.** Operators must publish a written data retention and deletion policy describing the purpose, business need, and deletion timelines of children's personal information. Indefinite retention of children's personal information is prohibited.

3. **Retention period.** Operators must retain children's information only as long as reasonably necessary to fulfill the specific purpose for which it was collected.

9 See 16 CFR § 312.2
10 See 16 CFR § 312.8
11 See 16 CFR § 312.4(c)(1)(vii)

d. Age Screening / Hyperlinks

1. **Mixed-audience exception.** A mixed-audience website or online service is not considered directed to children if it (i) does not collect personal information from any visitor prior to collecting age information; and (ii) prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the COPPA notice and verifiable parental consent provisions.
2. **Neutral age screening.** Operators must ask screening questions in a neutral manner so as not to encourage inaccurate answers from children trying to avoid parental permission requirements.
3. **Technical controls.** Age-screening mechanisms should be used in conjunction with technology (e.g., session cookies and other reasonable measures) to help prevent underage children from going back and changing their age to circumvent protections.
4. **Hyperlinks.** A website or online service is not considered directed to children solely because it refers or links to a commercial website or online service directed to children, or to a general-audience website. Similarly, a website directed to children is not considered in violation of these Guidelines by linking to a general audience website.