CARU Safe Harbor Program Requirements

The Children's Advertising Review Unit (CARU) was founded in 1974 to promote responsible children's advertising as part of a strategic alliance with the major advertising trade associations through the National Advertising Review Council (comprising the AAAA, the AAF, the ANA and the CBBB). CARU is the children's arm of the advertising industry's self-regulation program and evaluates child-directed advertising and promotional material in all media to advance truthfulness, accuracy and consistency with its *Self-Regulatory Guidelines for Children's Advertising* and relevant laws. As an extension of its mission, to help advertisers deal sensitively with the child audience in a responsible manner, CARU has established this Safe Harbor Program to aid our supporters in protecting the privacy of children online, and meeting the requirements of COPPA and our *Guidelines.*

CARU's Safe Harbor Program includes the following components:

Participant's full adherence to the requirements set forth in the CARU Safe Harbor Compliance Checklist;

Participant's compliance with CARU's *Self-Regulatory Guidelines for Children's Advertising*, including the Guidelines for Interactive Electronic Media;

Review by CARU staff of the participant Web site's information practices, including completion by CARU staff of an Initial Website Review and Seeding Form;

Ongoing monitoring and seeding by CARU staff of the participant's Web site to assess and ensure compliance with the Safe Harbor Program; and

Completion of CARU's Self-Assessment Form and Attestation by the Safe Harbor participant, which must be completed and signed by a responsible corporate officer, and the subsequent submission to CARU of an updated Self-Assessment Form and Attestation on each anniversary of the date of acceptance in the CARU Safe Harbor Program.

In addition, the participant agrees to be subject to the provisions of the *NAD/CARU/NARB Procedures*, including those concerning complaints, appeals and enforcement of compliance.

CARU Safe Harbor Compliance Checklist

PROVIDE NOTICE

All notices must be clearly written, understandable and contain no unrelated, confusing or contradictory materials.

1. Notice/Disclosure of Information Practices (Web Site Notice/ Children's Privacy Policy)

Operators of web sites directed to children or of general audience web sites that have a separate children's area, must post a prominent link, which must be clearly labeled as a Privacy Policy, Notice of Information Practices, Privacy Notice, or other, similar description to a notice of its information collection and use practices. The link to the notice must appear on the site's home page and at each area where personal information is collected from children, and must be placed in a clear and prominent manner on the home page and in close proximity to every place children directly provide, or are asked to provide, personal information. Operators of general audience web sites that have separate children's areas must post a link to a notice of its information practices with regard to children on the home page of the children's area.

The notice must state the following:

- The name, address, telephone number, and email address of all operators collecting or maintaining personal information from children through the web site. However, if more than one operator is responsible for a site, one operator may be designated as to respond to inquiries from parents concerning privacy policies and the use of children's information, as long as the names of all operators collecting or maintaining personal information from children through the web site are also listed in the notice;
- The types of personal information collected from children (for example, name, address, phone number, email address, etc.) and whether collected directly or passively (for example, through cookies);
- How the personal information is or may be used (for example, marketing back to the child, notifying contest winners, allowing the child to post personal information in chat rooms, bulletin boards, personal home pages or personal profiles);
- Whether the operator discloses any of the information collected from children to third parties. If such disclosure is made, the operator must disclose the types of businesses in which the third parties are engaged, the purposes for which the personal information is used, and whether each of the third parties have agreed to maintain the security and confidentiality of the information;
- That the parent has the option to agree to the collection and use of her child's information by the operator without consenting to the disclosure of that information to third parties;
- That the operator may not require the child to disclose more information than is reasonably necessary to participate in the activity as a condition of participation;
- That the parent can review the child's personal information, ask to have it deleted, and refuse to allow any further collection or use of the child's information. The notice also must provide the procedures for the parent to follow.

2. Direct Notice to Parents

Except as specifically authorized by the Rule (see below, Exceptions to Verifiable Parental Consent), before collecting personal information from children, operators must notify parents of the operator's information collection and disclosure practices. The notice to parents must state the following:

- All the same information included in the notice on the web site (use of a link to the web site notice is acceptable);
- That the operator wishes to collect personal information from the child;
- That the parent's consent is a prerequisite for the collection, use or disclosure of the information;
- The method(s) for providing parental consent.

OBTAIN VERIFIABLE PARENTAL CONSENT

An operator must obtain verifiable parental consent before collecting, using or disclosing personal information from a child, except as specifically authorized by the Rule. The consent may be obtained as follows:

- When personal information is collected for internal use only, such as marketing back to a child, the operator may use email to obtain parental consent, as long as the operator takes additional steps, such as follow-up email, letter or phone call, to verify that the parent, in fact, has provided the consent.
- When operators make personal information publicly available (for example, through a chat room, message board, personal home page, personal profile, email account) or disclose the information to third parties, operators must use one of the "more reliable" methods of obtaining parental consent such as one of the following:
  a) obtain a signed form from the parent via postal mail or facsimile;
  b) obtain and verify a credit card number in connection with a transaction;
  c) set up a toll-free phone number staffed by trained personnel;
  d) obtain email consent coupled with a digital parental signature;
  e) obtain email consent accompanied by a PIN or password acquired through one of the above-noted verification methods;
  f) obtain consent through any method, approved by CARU, that is reasonably calculated, in light of available technology, to ensure that the person providing the consent is the child's parent.

After April 21, 2002, only the "more reliable" methods of obtaining parental consent may be used by operators.

The operator must give the parent the option to agree to the collection and use of the child's personal information without agreeing to disclosure of that information to third parties.

Information collected about a parent, whether from children or parents, for the purpose of obtaining verifiable parental consent or providing notice, should not be maintained in

retrievable form by the site if parental consent is not obtained after a reasonable time, and, even if parental consent is obtained, should not be used for any other purpose.

An operator is required to send a new notice and request for consent to parents if there are material changes in the collection, use or disclosure practices to which the parent had previously consented.

Exceptions to Verifiable Parental Consent

Prior parental consent is not required under the following circumstances:

- When an operator collects a child's or parent's email address to provide notice and seek consent;
- When an operator collects a child's email address to respond to a one-time online request from a child, uses the email address once for that specific purpose, and then deletes it;
- When an operator collects a child's email address to respond more than once to a child's specific online request (such as for an email newsletter or contest). In such instances, the operator must provide direct notice to the parent. The direct notice must contain all the information set forth in the privacy policy and must notify the parent that the operator is communicating regularly with the child online, identify the nature and intended uses of the information and give the parent the opportunity to stop the communication before sending or delivering a second communication to the child. The direct notice must inform the parent that if the parent does not opt out, the operator may use the email address for the purpose stated in the notice. The operator must permit parental access to the information sufficient to permit the parent to remove or correct the information. The operator cannot use the information for any other purpose.
- When an operator collects a child's name and/or online contact information to protect the safety of a child who is participating on the site. In this case, the operator must provide direct notice to the parent. The direct notice must contain all the information set forth in the privacy policy and must notify the parent that the operator has collected the child's name and email address to protect the safety of the child participating on the website and that the parent may refuse to permit the use of the information, may require its deletion and the method to do so. The direct notice must inform the parent that if the parent does not opt out, the operator may use the email address for the purpose stated in the notice. The operator cannot use the information for any other purpose.
- When an operator collects a child's name and/or online contact information to protect the security of the site, to take precautions against liability, to respond to judicial process, or as permitted or required to respond to law enforcement or public safety investigations, and does not use it for any other purpose.

LIMIT THE COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION COLLECTED FROM CHILDREN

Operators of Web sites cannot condition a child's participation in a game, the offering of a prize or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity and instead, must limit the collection of personal information from a child to only that which is reasonably necessary for the child's participation in an activity.

In addition, the Web site operator must give the parent the option to consent to the collection and use of the child's personal information without consenting to the disclosure of that information to third parties.

PROVIDE ACCESS UPON VERIFICATION OF PARENTAL IDENTITY

Operators of web sites**,** when requested by parents, must disclose to parents the types of information they collect from children (for example, name address, phone number, email address, hobbies etc,) as well the specific information collected. In addition, operators must give parents the opportunity, at any time, to refuse to permit the operator's further use or future online collection of personal information from her child, and to direct the operator to delete the child's personal information. In order to ensure that operators do not disclose a child's specific personal information to someone who is not the child's parent the operator must verify the parent's identity using one of the following methods:

- obtain a signed form from the parent via postal mail or facsimile;
- obtain and verify a credit card number in connection with a transaction;
- set up a toll-free phone number staffed by trained personnel;
- obtain email coupled with a digital parental signature;
- use any method approved by CARU that ensures that the requestor is the parent of that child, taking into account available technology;
- obtain email accompanied by a PIN or password acquired through one of the above-noted verification methods.

MAINTAIN REASONABLE SECURITY

Operators of web sites must establish procedures and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. This includes, for example, limiting employee access to data, deleting personal information when no longer used, physical security of servers, encryption of data during transmission, use of firewalls, etc.