ENTERTAINMENT SOFTWARE RATING BOARD
317 MADISON AVENUE 22ND FLOOR NEW YORK, NY 10017 212 759 0700 | FAX 212 759 2223
WWW.ESRB.ORG

ESRB KIDS PRIVACY ONLINE SEAL REQUIREMENTS

The ESRB Kids Privacy Online Seal Requirements apply if any part of your website is directed to children under 13 (12 years and younger), or if you have actual knowledge that you collect personal information from children under 13. Federal law requires such a website to comply with the requirements of the Children's Online Privacy Protection Rule (16 C.F.R. Part 312). ESRB's Kids Privacy Online Seal Requirements may be modified as necessary to meet the requirements of the Children's Online Privacy Protection Act ("COPPA"). ESRB Kids Privacy Online Seal Requirements have been approved by the Federal Trade Commission as an authorized COPPA "Safe Harbor."

If you operate a website or online service directed to children under 13 years old, you must assume your visitors are under 13 years old. The COPPA Rule offers the following factors to determine if a website is directed to children under 13 years old. In determining whether a website is directed to children, we will look at the overall character of your website, and not just the presence or absence of one or more factors.

- Subject matter
- Visual or audio content
- Age of models
- Language or other characteristics of the website
- Advertising promoting or appearing on the website is directed to children
- Competent and reliable empirical evidence regarding audience composition
- Evidence regarding intended audience
- Whether website uses animated characters and/or child-orientated activities and incentives

If you operate a general audience website, you may assume your visitors are not children under 13 years old, unless you have actual knowledge that a visitor is a child. If you operate a "mixed appeal" or "tween" website, which appeals to both children and teens, you must ask the age of the visitor in a neutral manner, take reasonable steps to prevent children under 13 years old from claiming to be older than they are, and apply appropriate information practices. Though a request that visitors identify their age may, in certain cases, not yield totally accurate results, if you ask age in a neutral manner, you may rely on the age given.

I. PRIVACY STATEMENT REQUIREMENTS

Your Privacy Statement must be clear and understandable, and should not include any unrelated, contradictory, or confusing information. It should be easy to read with no animated graphics, advertisements, or any distracting marketing materials. It must include:

1. **Contact Information.** You must always list your complete contact information -- including a contact name, telephone number, postal address, and email address. In addition, you must also either: (i) list the complete contact information for every other person, organization, or

company collecting information through your website: or (ii) agree to respond to all privacy inquiries, as long as the names of all other persons, organizations, or companies collecting or maintaining personal information through your website are also listed in your Privacy Statement.

2. **Collection of Personal Information.** You must include the types of personal information collected and whether the information is collected directly or indirectly.

3. **Use of Personal Information.** You must indicate how children's personal information is used, including but not limited to whether it is used for fulfillment of a requested transaction, record keeping, marketing products or services back to the child, or publicly disclosing personal information in a chat room, bulletin board, or other online forum.

4. **Third-Party Disclosure and Parental Choice.** You must indicate whether you disclose personal information to third parties. If you disclose personal information to third parties, you must: (i) describe the types of business in which such third parties are engaged and the general purposes for which such information is used; (ii) indicate whether the third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from you; (iii) state that the parent has the option to consent to your collection and use of their child's personal information without consenting to your disclosure of that information to third parties; and (iv) describe the procedures for parents to prevent your disclosure of their child's information to third parties.

5. **Limiting Information Collection.** You must state that you are prohibited from conditioning a child's participation in an activity on the child disclosing more personal information than is reasonably necessary to participate in such activity.

6. **Parental Access.** You must state that parents may view and remove their child's personal information, and refuse to permit you to further collect or use their child's personal information. You must also describe the procedures for exercising parental access for any purpose, including to prevent the disclosure of their child's information to third parties.

II. KIDS SEAL POSTING REQUIREMENTS

You must prominently post the ESRB Privacy Online Children's Certification Seal ("Kids Seal") on the homepage of the website and in close proximity to each area where you collect personal information from children online ("information entry points"). If you operate a general audience website that has a separate children's area, you must prominently post the Kids Seal on the homepage of the children's area and in close proximity to any information entry points in the children's area. The Kids Seal must link directly to your Privacy Statement or, if you are a general audience website, the section of your Privacy Statement describing your information practices regarding children.

III. DIRECT NOTICE AND PARENTAL CONSENT REQUIREMENTS

1. Direct Notice to Parents to Obtain Prior Verifiable Parental Consent

You must make reasonable efforts, taking into account available technology, to ensure that a parent receives notice of your information practices, including notice of any material change in your information practices to which the parent has previously consented. With limited exceptions, you must provide notice to parents and obtain verifiable parental consent *before* collecting any personal information from a child. For exceptions to these requirements, see Section III.3 below.

Direct notice to parents sent to obtain prior verifiable parental consent must contain:

A. Privacy Statement Information. You must include all of the information that is required under Section I, above.

B. Intent to Collect Information. You must state that you wish to collect personal information from the parent's child and set forth the types of information you wish to collect.

C. Parental Permission Required. You must state that you are required to obtain the parent's permission to collect the personal information from the child. You must also describe the procedures by which a parent may give such permission.

2. Prior Verifiable Parental Consent

In most cases, you must obtain verifiable parental consent *before* you collect, use, or disclose a child's personal information. You must also obtain verifiable parental consent to any material change in your information practices to which the parent has previously consented *before* implementing such changes.

Mechanisms for Verifiable Parental Consent. You must take reasonable measures, in light of the available technology, to ensure that the person providing consent is the child's parent. Acceptable mechanisms for obtaining verifiable parental consent include: (i) providing a consent form to be signed by the parent and returned to you by mail or fax; (ii) requiring a parent to use a credit card *in connection with a transaction*; (iii) having a parent call a toll-free telephone number staffed by trained personnel; (iv) using an electronic (digital) signature; or (v) using e-mail accompanied by a PIN or password obtained through one of the verification methods described above.

Information you collect for internal use only. Where your use of information is internal and there is no disclosure to third parties or the public, methods to obtain prior verifiable parental consent may also include use of email, coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: sending a delayed confirmatory email to the parent after receiving consent; or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. If you use such methods, you must provide notice in the confirmation that the parent can

revoke any consent given in response to the earlier email and instructions on how to revoke consent.

3. Exceptions to Prior Verifiable Parental Consent

Although prior verifiable parental consent is required in most cases before you collect, use, or disclose a child's personal information, in a few exceptions you may collect a child's or parent's name or online contact information (i.e., email address) before obtaining parental consent. As detailed below, in some cases, you must send the parent a direct notice of your information practices containing specific statements about the information collection and use.

A. Obtaining Consent. You may collect the name or online contact information of a parent or child for the sole purpose of obtaining parental consent -- so long as you delete such information from your records if you have not obtained parental consent after a reasonable time from the date of information collection. To obtain parental consent, you must provide parents with a direct notice that includes all information set forth in Section III.1, above, and must explain that you have collected the name or online contact information of the parent or child to provide notice to and obtain consent from the parent. You must not use such information to recontact the child or the parent, or for any other purpose.

B. One-Time Response. You may collect online contact information from a child for the sole purpose of responding directly, on a one-time basis, to a specific request from the child -- so long as such information is not used to recontact the child or for any other purpose, and is subsequently deleted from your records. Under this exception, you do not need to provide direct notice to parents or obtain verifiable parental consent.

C. Multiple Responses. You may collect the online contact information of a child and parent to be used to respond directly, more than once, to a specific request from the child -- so long as such information is not used for any other purpose. In such cases, you must make reasonable efforts, taking into consideration available technology, to give direct notice to parents, which must: (i) include all Privacy Statement information (see Section I, above); (ii) explain to the parent that you have collected the child's online contact information to respond to the child's request; (iii) explain that the child's request will require more than one contact with the child; (iv) explain that the parent may refuse to permit further contact with the child and may require you to delete the child's information; (v) explain how a parent can refuse to permit further contact and information collection from the child; and (vi) explain that if the parent does not respond, you may use the information for the purposes stated in the direct notice. This direct notice to parents must be sent immediately after your initial response to the child and before sending any additional response.

D. Protecting Child Safety. You may collect a child's name and online contact information to the extent reasonably necessary to protect the safety of a child participant on the website where you have used reasonable efforts to provide notice to the parent -- so long as such information is used for the sole purpose of protecting the child's safety, not used to re-contact the child or for any other purpose, and not disclosed on the website. In such cases, you must make reasonable efforts, taking into consideration available

technology, to give direct notice to parents, which must: (i) include all Privacy Statement information (see Section I*,* above); (ii) explain that you have collected the child's name and online contact information to protect the child's safety; (iii) explain that the parent may refuse to permit further contact with the child and may require you to delete the child's information; (iv) explain how a parent can refuse to permit further contact and information collection from the child; and (v) explain that if the parent does not respond, you may use the information for the purposes stated in the direct notice.

E. Protecting Others. You may collect a child's name and online contact information to protect the security or integrity of your website, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or investigations on matters related to public safety — so long as such information is not used for any other purpose. Under this exception, you do not need to provide direct notice to parents.

IV. PARENTAL ACCESS REQUIREMENTS

You must provide parents reasonable access to their child's personal information. Such access must include: (i) a description of the types of information you collect from children, such as name, address, telephone number, and hobbies, and the specific information you have collected from their child; (ii) the opportunity to prevent you from further using or collecting information about their child in the future; and (iii) the opportunity to direct you to delete their child's personal information from your records. You must take reasonable measures, in light of the available technology, to ensure that the person requesting access is the child's parent. Acceptable verification mechanisms include: (i) providing a request form to be signed by the parent and returned to you by mail or fax; (ii) requiring a parent to use a credit card *in connection with a transaction;* (iii) having a parent call a toll-free telephone number staffed by trained personnel; (iv) using an electronic (digital) signature; or (v) using email accompanied by a PIN or password obtained through one of the verification methods described above. Acceptable methods for verifying a parent's identity over the telephone may include asking a series of questions that only the parent would know (e.g., parent's name, postal address, email address, child's name and email address, security question taken at sign up, etc.).

V. LIMITING INFORMATION COLLECTION REQUIREMENTS

You are prohibited from conditioning a child's participation in an activity on the child disclosing more personal information than is reasonably necessary to participate in such activity.

VI. DATA INTEGRITY AND SECURITY REQUIREMENTS

You must establish and maintain reasonable procedures, taking into account available technology, to protect the confidentiality, security, and integrity of personal information collected from children.

VII. OVERSIGHT REQUIREMENTS

1. License Agreement

You must execute and be bound by the ESRB Privacy Online License Agreement. As part of this Agreement and as a material obligation, you must agree to comply at all times with all aspects of the ESRB Kids Privacy Online Seal Requirements. Failure to comply with any of the Seal Requirements could be interpreted by ESRB as a material breach of the Agreement and constitute a trademark infringement and a dilution of the goodwill and reputation attaching to ESRB's mark.

2. Privacy Statement Assistance

ESRB will assist you in creating or modifying your Privacy Statement. If you do not have a Privacy Statement, ESRB will help you create one. ESRB is available to work with you to ensure that your Privacy Statement reflects your information practices and adheres to all of ESRB's requirements.

3. Self Evaluation

You must complete ESRB's "Self Assessment Questionnaire" describing your privacy practices in preparation for the Onsite Audit and annually thereafter. You must complete this questionnaire diligently and in good faith, and sign and attest that all the statements made are true and accurate as of the date submitted.

4. Onsite Audit

Prior to certification, you must submit to an ESRB Onsite Audit. Each Onsite Audit is conducted by a staff attorney who is trained in the area of privacy law. Through these onsite audits, ESRB determines whether your privacy statement is an accurate representation of your internal and external information practices. The Onsite Audit also provides ESRB with the opportunity to ensure that your information practices meet all of ESRB's Kids Privacy Online Seal Requirements and maintain them on a consistent basis. ESRB does not grant your certification without first conducting an Onsite Audit showing that you meet the program's criteria.

5. Monitoring and Verification

You must submit to quarterly reviews of your information practices. The goal of these reviews is to provide effective ongoing enforcement and assure both the consumer and you that a reliable safeguard exists to verify that your privacy policy implementation is accurate, meaningful, and effective. Monitoring reviews are unannounced and conducted by specially trained online monitors methodically moving through your website, page by page, ensuring that you comply with all aspects of the ESRB Kids Privacy Online Program.

If ESRB discovers a possible violation regarding your information practices, we will flag the matter in a Monitor's Report. An ESRB Compliance Manager reviews these reports, and confirms whether there is a possible violation. The Compliance Manager then notifies you that an inquiry into your information practices is being initiated and that, depending on the

determination, further action may be required. If ESRB determines that a violation of the Seal Requirements has occurred, you are notified in writing of the specific violations, the corrective actions you must take to address the violations, and the consequences of failing to take such actions. Failure to take the corrective actions can result in a number of penalties including: the imposition of fines; removal of the Kids Seal; and referral to the Federal Trade Commission (see Outside Agency Referral, below). Penalties are assessed according to the type of violations and whether such violations were inadvertent, intentional, or willful. In addition, penalties may be assessed against companies that exhibit a pattern of non-compliance.

6. Spot Checks

You must submit to randomly scheduled, unannounced audits of your privacy practices, known as "Spot Checks." Spot Checks involve the seeding of your database by ESRB, which submits fictitious consumer data at each information entry point. Your response is then tracked and recorded to determine if your information practices adhere to your Privacy Statement.

7. Consumer Online Hotline

The Consumer Online Hotline is a no-charge service that allows consumers who have a privacy grievance or who believe that a privacy violation has taken place on your website to directly report the violation or grievance to ESRB. The reporting can be done swiftly and easily by filling out the Consumer Online Hotline form, indicating the alleged privacy violation. ESRB responds immediately to all consumer concerns and complaints submitted in any form.

8. Alternative Dispute Resolution

You must create and implement an internal dispute resolution program, which should be designed to fairly and expeditiously resolve privacy related issues and complaints raised by either consumers or ESRB. In addition, you must submit to ESRB Privacy Online's Alternative Dispute Resolution services when consumer grievances are not effectively addressed through your company's own internal mechanisms. You are required to fully participate in any inquiry or investigation opened by ESRB Privacy Online, and are bound to abide by the final judgment of any ESRB Alternative Dispute Resolution.

9. Outside Agency Referral

If you fail to take appropriate actions in response to a valid complaint or an ESRB mandate, or in any way engage in a pattern of violating ESRB Kids Privacy Online Seal Requirements, ESRB may invoke the remedies described above and refer you to the Federal Trade Commission for engaging in unfair and deceptive trade practices.

VIII. ORGANIZATIONAL REQUIREMENTS

1. Compliance Mechanisms

You must create and implement internal processes for ensuring that you comply with your Privacy Statement and other privacy practices. You must train personnel who are in a position to collect personal information from or about children to adhere to your Privacy Statement and

other privacy practices. You must assign specific personnel the responsibility for monitoring compliance with your Privacy Statement and other privacy practices. You must create a system of incentives and/or sanctions to encourage adherence to your Privacy Statement and other privacy practices.

2. Verification Mechanisms

You must also verify that the assertions you make about your privacy practices are true and that privacy practices have been implemented as represented. Children's personal information is always considered highly sensitive, and we will hold you to a higher standard of verification. To this end, you must regularly review your compliance with your stated privacy practices.

3. Complaint Mechanisms

You must also create and implement internal processes affording consumers appropriate means of recourse for claimed failures by you to adhere to your stated privacy practices. Appropriate means of recourse include, at a minimum, institutional mechanisms to ensure that consumers have a simple, effective way to have their concerns addressed.

For example, you must appoint identifiable, accessible, and responsive personnel to whom consumers can bring a grievance initially. You must give such personnel the authority to investigate the grievance in a timely manner. Such personnel must be required to submit a written response to the aggrieved consumer that details the results of the investigation, and should be given incentives to respond to consumers in a timely manner.

If you have not adhered to your privacy practices, you must offer consumers a remedy for your violation. Such a remedy must be appropriate under the circumstances of the case and may include the righting of the wrong (e.g. correction of any misinformation, cessation of further collection of personal information from that consumer, or deletion of improperly collected personal information) or compensation for any harm caused.

If the consumer is not satisfied with the resolution, you must provide the consumer with a mechanism to appeal initial decisions to higher management levels.

Lastly, if the consumer is still unsatisfied regarding the resolution of a grievance, the consumer must be referred to ESRB Alternative Dispute Resolution Officer (see Alternative Dispute Resolution, Section VII.8 above).