ENTERTAINMENT SOFTWARE RATING BOARD

March 13, 2018

Via Electronic Mail and First Class Mail
Mr. Donald S. Clark
Office of the Secretary
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC
secretary@ftc.gov

Re: Amended Submission of the Entertainment Software Rating Board's Proposed Post-Approval Modifications to its ESRB Privacy Certified Kids Seal Requirements under 16 CFR § 312.11(e)

Dear Mr. Clark,

I write on behalf of the Entertainment Software Rating Board ("ESRB") to request approval of the ESRB's proposed modifications to our Privacy Certified Kids Seal Program (the "Program") requirements from the Federal Trade Commission (the "Commission"). This letter reflects a slight modification to my initial letter dated January 26, 2018, which modification is based on my communications with the Commission's staff.

ESRB operates one of the first safe harbor programs under the Children's Online Privacy Protection Act ("COPPA"), having received approval from the Commission in 2001. The Program requirements (the "Requirements") were last amended in 2013, in response to the Amended COPPA Rule. We believe it is important to continuously assess the Requirements to ensure they remain current with the Commission's COPPA-related regulations and guidance, and to allow ESRB to monitor and uphold compliance with the Requirements in the most efficient and effective manner. With that in mind, I am enclosing:

- Under Exhibit A, our proposed Privacy Certified Kids Seal Program Requirements (the "Proposed Requirements") for which we are seeking the Commission's review and approval under 16 CFR § 312.11(e); and

- Under Exhibit B, a blackline draft of the Proposed Requirements, showing all proposed changes to the Program's existing Requirements.

Pursuant to 16 CFR §§ 312.11(c)(2) and (e), the following is a description of how the proposed changes affect the Program's existing Requirements. This statement does not include non-substantive changes, for example changes in terminology (all of which are reflected in Exhibit B).

420 LEXINGTON AVENUE SUITE 2240 NEW YORK, NY 10170
212 759 0700 | FAX 212 759 2223 WWW.ESRB.ORG

- In Section I of the Proposed Requirements, we have revised the definition of the term "Personal Information and Data" to more closely track the Amended COPPA Rule and Commission guidance. For example, within the definition of "Personal Information and Data," we have clarified that audio recordings are not included if they are used solely to effectuate speech-to-text functionality and are deleted immediately thereafter. That change is consistent with the Commission's October 23, 2017 COPPA guidance. We have also made explicit that personal information and data includes personal information and data contained within the metadata of a photograph, video recording or audio recording.
- In Section I of the Proposed Requirements, we have removed the definition of the term "Privacy Risk Assessment" because that term was not otherwise utilized in the Program Requirements.
- In Section II of the Proposed Requirements, for new participants in the Program, we have removed the requirement for an initial Self-Assessment Questionnaire ("SAQ") to be completed prior to or upon joining the Program. This requirement, which is currently found in Section II.A., is no longer necessary. Instead, especially in the early stages of membership, we have found that Program participants benefit from a more personal approach, usually involving at least one (but more likely several) telephone calls or video conferences to introduce them to the Program and to allow us to gather necessary information. However, we have reserved the right to require an SAQ at other times, if necessary.
- Moreover, in Section II.A. of the Proposed Requirements, we have clarified certain aspects of the initial Compliance Report, including that ESRB will provide participants with required and suggested changes to their privacy statements.
- We have removed the requirement for an initial Onsite Compliance Review for new participants, which is currently found in Section II.B. Program participants are located throughout the United States and even outside the United States. We do not believe they should be burdened by the time and expense of an initial Onsite Compliance Review when we can accomplish the same objectives and gather the same information through video conferences, telephone conferences, and correspondence.
- We have revised Section II.B. of the Proposed Requirements (currently Section II.C.) to clarify that new members will get at least one Compliance Report in their initial term. This change is necessary because some members join later in our fiscal year, thereby shortening their initial terms. If, for example, a member was to join in December, we likely would provide that member with a single compliance report in its initial term, rather than two or more.
- In Section III.C. of the Proposed Requirements, we have removed the second sentence because it is redundant of the first sentence. We have also removed the qualifying language "in the next scheduled Compliance Report" from the final sentence of that

Section because time could be of the essence, in which case we would notify the participant of our discovery as soon as possible.

- In Section III.D.2. of the Proposed Requirements, we have changed "maintain a consumer online hotline" to "provide contact information on its website," to clarify that ESRB does not maintain a telephone hotline. Rather, consumers submit inquiries and complaints to us via email at privacy@esrb.org.
- We have made several changes in Sections IV.A. and IV.B. of the Proposed Requirements to strengthen the disclosures in participants' privacy statements.
- In Section IV.C. of the Proposed Requirements, we have clarified that the link to a Kids Privacy Statement must be prominent and clearly labeled, and we have added the requirement for online apps that a link to the privacy statement be available in the app store prior to download.
- In Section V.A. of the Proposed Requirements, we have made minor revisions to strengthen the disclosures in direct notices to parents.
- In Section V.B. of the Proposed Requirements, we have added the use of approved vendors, such as Veratad Technologies, to the list of available mechanisms to obtain verifiable parental consent.
- In Section VII.A. of the Proposed Requirements, consistent with the best practice of data minimalization, we have added text to make clear participants should not collect personal information and data if it is not being utilized.
- In Section VII.E. of the Proposed Requirements, we have changed "must" to "should" to clarify that this requirement is a recommended best practice, as opposed to an obligation under COPPA or the Amended COPPA Rule.

* * *

We look forward to the Commission's review and consideration of the Proposed Requirements. If I can be of any assistance during that process, please contact me at (917) 522-3267 or jfalzone@esrb.org.

Sincerely,

John Falzone

John M. Falzone, Esq.
Vice President, ESRB Privacy Certified

Enclosures

EXHIBIT A

Proposed ESRB Privacy Certified Kids Seal Requirements

If a Monitored Product is directed or targeted at children under the age of thirteen (13) *or* Participant has actual knowledge it is collecting or maintaining (or allowing a third party to collect or maintain) personal information or data from children under the age of thirteen (13) through a Monitored Product, then Participant must comply with the ESRB Privacy Certified Kids Seal Requirements set forth in this Schedule for all such Monitored Products Participant has submitted to ESRB for certification and on which Participant intends to display the Privacy Certified Kids Privacy seal and/or the ESRB Privacy Certified Mobile seal.

I. DEFINITIONS

Child/Children means users resident in the United States who are under thirteen (13) years of age.

Online Information Practices encompass, but are not limited to: (i) Participant's practices regarding consumer notification and consumer access to their Personal Information and Data (as that term is defined below); (ii) Participant's practices with respect to the collection, use or disclosure of Personal Information and Data; (iii) Participant's practices regarding user choice and consent to how Personal Information and Data is used or shared; and (iv) security measures taken to protect Personal Information and Data provided by users.

Personal Information and Data ("PID") means any information relating to an identified or identifiable individual collected online, including, but not limited to:

- First and last name;
- Home or other physical address or geolocation information;
- Online contact information (*e.g.*, email address, instant messenger identifier, video chat identifier, VOIP identifier, and screen name that permits direct contact with the individual online);
- Phone number;
- Persistent identifier (*e.g.*, a customer number held in a cookie, internet protocol address, device serial number, or unique device identifier), if additional PID is collected and/or the persistent identifier(s) are not used solely to support the internal operations of the Monitored Product;
- Photograph or video recording showing the individual's face or otherwise containing PID in the photograph or recording or within the metadata of the photograph or recording;
- Audio recording capturing the individual's voice or otherwise containing PID within the recording or the metadata of the recording, except to the extent such audio recordings are used solely to effectuate speech-to-text functionality in the Monitored Product and deleted immediately thereafter; and
- Social security number or other government identification number.

Demographic information (including, but not limited to, gender, age, date of birth, educational background, or political affiliation) also becomes PID when combined with other information enabling the individual to be identified. PID does not include information that is rendered anonymous.

Privacy Statement means the statement, posted on the Monitored Products, which discloses Participant's up-to-date policies regarding user privacy and Participant's practices with respect to the collection, use and disclosure of PID.

II. PROGRAM DOCUMENTS AND PROCEDURES

A. Initial Compliance Report

ESRB shall review Participant's Privacy Statement and related Online Information Practices with respect to the Monitored Products. ESRB shall assess the state of Participant's overall compliance with the Program Requirements after which it shall provide Participant (i) required and suggested changes to Participant's Privacy Statement; and (ii) a comprehensive report detailing any and all required and suggested changes to Participant's Online Information Practices with respect to the Monitored Products ("Compliance Report").

Participant shall implement all changes required to the Privacy Statements and by the Compliance Report and attest to ESRB that it has done so in writing. ESRB shall then complete a final review of the Privacy Statement and Monitored Products. If all the required changes have been implemented or otherwise resolved, ESRB shall provide Participant with written approval to use and access to the appropriate Program Marks.

B. Biannual Monitoring and Compliance Reports

At least once during the Initial Term and no more than twice during each Renewal Term ("Reporting Periods"), ESRB shall provide Participant with a Compliance Report that will: (i) list all of the Monitored Products; (ii) describe changes to Participant's Privacy Statement and/or Monitored Products that are necessary for Participant to remain compliant with the Kids Seal Requirements; and (iii) propose changes which, although not required under the Kids Seal Requirements, reflect "best practices" that are highly recommended by ESRB. Within three (3) weeks of Participant's receipt of a Compliance Report, Participant must notify ESRB, through ESRB's SharePoint system (or through whatever other means may be specified by ESRB pursuant to its then-current policy), that Participant has implemented all changes required by the Compliance Report. If Participant needs more than three weeks to implement the required changes, Participant shall notify ESRB immediately and provide a time frame within which it commits to complete all changes.

For ESRB to provide thorough and accurate Compliance Reports, Participant must provide ESRB full access to the Monitored Products, including access to "members only" or password-protected areas of the Monitored Products.

III. CONTINUING OBLIGATIONS OF PARTICIPANT

A. Designation of Site Coordinator

Participant shall name a coordinator for the Monitored Products ("Site Coordinator") who shall be ESRB's primary contact. Participant shall notify ESRB in the event of a change to the individual designated as Site Coordinator. The Site Coordinator shall be responsible for the effectuation and implementation of Participant's Online Information Practices reflected in its Privacy Statement and compliance with the Kids Seal Requirements. All notices from ESRB shall be directed to the Site Coordinator.

B. Notifying ESRB of Material Changes

1. Participant shall notify ESRB in advance of any material change(s) to its Online Information Practices, including, by way of example, changes to Participant's Terms of Use or End User License Agreement; changes to its data security infrastructure; or the roll-out of any new sweepstakes, contest or similar promotion through the Monitored Products.

2. Participant shall obtain prior approval from ESRB for all substantive modification to its Privacy Statement, whether such modification results from a material change in Participant's Online Information Practices, the revamping of Monitored Products, or otherwise.

3. Where changes to Participant's Monitored Products, Privacy Statement or Online Information Practices have been implemented, Participant may be required to submit a Self-Assessment Questionnaire ("SAQ") or provide updated information in a form determined by ESRB. Participant may also be required to submit a SAQ if Participant has undergone a change in control, or if there has been an investigation of Participant's practices by a federal or state authority, agency or regulatory body or any unit of federal or state government.

C. Notifying Users of Material Changes

Participant shall notify users of any material change(s) in its Online Information Practices or Privacy Statement. Notice should be provided to users prior to the change taking effect. Different types of material changes may require different forms of notice to users. If, while reviewing Participant's Monitored Products in the normal course, ESRB discovers a material change of which it was not previously notified, ESRB will advise Participant of the type of notice Participant must provide to users of the Monitored Products.

D. Resolution of Consumer Complaints

1. Participant shall implement procedures to receive, investigate and resolve privacy inquiries and complaints from users. Where Participant's internal mechanisms are unable to address a user grievance effectively, Participant shall refer the user to ESRB for dispute resolution.

2. ESRB shall provide contact information on its website, which visitors to Participant's Monitored Products may use to contact ESRB with inquiries or complaints regarding a Monitored Product. After determining the nature of the complaint, ESRB shall respond in one of the following ways.

a. If the question, concern or complaint is not privacy-related, ESRB shall either forward it to the individual at Participant's company designated for such purpose or redirect the consumer to the appropriate contact mechanism (e.g., support page).

b. If the inquiry or complaint is privacy-related and presents a question or an issue ESRB can independently address, ESRB shall respond directly to the consumer.

c. If the inquiry or complaint is privacy related, but requires information or input from Participant, ESRB shall contact Participant. Participant shall cooperate with ESRB in resolving consumer complaints.

3. If neither Participant nor ESRB succeeds in independently resolving a consumer grievance, and the consumer wishes to pursue the matter further, Participant agrees to fully participate, along with the consumer, in a dispute resolution process conducted by ESRB and agrees to accept ESRB's judgment as final.

E. Required Notice to ESRB

Participant shall notify ESRB in writing within thirty (30) days if Participant: (i) changes its name; (ii) undergoes a change in control; or (iii) changes the domain name of any Monitored Product.

IV. PRIVACY STATEMENT

A. Content of General Privacy Statement

Participant shall maintain and abide by a Privacy Statement that is either written by Participant and approved by ESRB, in its sole discretion, or written by ESRB. The Privacy Statement shall clearly set forth Participant's Online Information Practices. The Privacy

Statement must link only to and from web pages that are in the English language. If a Participant wishes to link the Privacy Statement to or from a web page or mobile application in a language other than English, the Privacy Statement must be translated and localized for the applicable language/locality. At a minimum, Participant's posted Privacy Statement shall provide disclosure to users with respect to each of the following elements:

1. Notice that the Monitored Product has been reviewed and certified by the ESRB Privacy Certified Program;
2. A full description of how users can contact Participant, including the Participant's name, postal address, and email address;
3. A full description of how users can contact ESRB with questions or concerns about Participant's Privacy Statement or Online Information Practices;
4. A complete list of all PID collected through the Monitored Product, how each PID identified is collected, and how it is used;
5. The identity (including name, address and e-mail address) of all entities that are collecting or maintaining PID on behalf of or through the Monitored Product;
6. The entities (if any) with whom PID collected through the Monitored Product is shared or disclosed, including the types of businesses in which any third parties are engaged, the general purpose for which the information is used by the third parties, and whether the third parties have agreed to maintain the confidentiality, security, and integrity of the PID collected by Participant;
7. Notice of whether Participant supplements PID collected through the Monitored Products with information from other sources and, if so, a description of the PID and the sources from which they were collected;
8. Disclosure of the tracking technologies, if any, used on the Monitored Product either by Participant or by an authorized third party;
9. An explanation of when and how users may exercise opt-in and/or opt-out options, including the choices available to them regarding how their PID is collected and used;
10. The nature of the security measures in place on the Monitored Products;
11. Notice that PID provided to Participant may be subject to disclosure in response to judicial or other government subpoenas, warrants, or orders;
12. Notice that information posted by users in online bulletin boards, chat rooms, news groups, or other public forums may be displayed publicly;
13. The notification procedures to be utilized by Participant in the event of a material change in its Online Information Practices and/or Privacy Statement; and
14. Disclosure of the effective date or last date on which the Privacy Statement was updated (i.e., "updated as of").

B. Content of Kids Privacy Statement

If Participant is collecting PID from Children, or if any portion of Participant's Monitored Products are directed to or target Children, then Participant either must implement a separate Kids Privacy Statement, or incorporate into its General Privacy Statement a section specifically devoted to Participant's Online Information Practices with respect to Children.

In addition to the elements set forth in Section IV.A. above, Participant's Kids Privacy Statement, or, if there is no separate Kids Statement, that portion of Participant's General Privacy Statement reflecting its Online Information Practices with respect to Children, must contain the following elements:

1. Disclosure of the manner in which Children's PID is collected through the Monitored Product and how it will be used (*e.g.*, to fulfill a requested transaction, for record keeping purposes, for the purpose of marketing products or services to Children, etc.);

2. Notice that a Child's participation in a chat room, bulletin board, or other online forum provided by Participant may result in such Child's public disclosure of PID, and notice of Participant's policy to remove any such PID if and when discovered;

3. Notice that a parent has the option to consent to Participant's collection and use of their Child's PID without consenting to Participant's disclosure of that information to third parties;

4. A description of the procedures pursuant to which parents can prevent Participant's disclosure of their Child's PID to third parties;

5. Disclosure that Participant may not condition a Child's participation in an activity on such Child's disclosing more PID than is reasonably necessary to participate in such activity;

6. Notice that parents may refuse to allow Participant and/or any third party from further collecting or using their Child's PID;

7. A description of the process by which a parent can, for any purpose, access, correct, or delete their Child's PID; and

8. A description of the process by which third parties give parents access to review, correct, or delete their Child's PID, including for the purpose of preventing disclosure to third parties of their Child's PID.

C. Placement of Kids Privacy Statement and Other ESRB Marks

Participant must provide, on its home page and on any pages where PID is collected from Children, a prominent and clearly labeled link to its Privacy Statement. If the Monitored Product is a website, Participant should post the "Kids Privacy Seal" Mark near the link to the Privacy Statement. The Kids Privacy Seal Mark must link directly to Participant's membership confirmation page hosted at esrb.org.

If the Monitored Product is an online app, a link to the Privacy Statement must be in the app store, available prior to download. A Privacy Statement, preferably a short form template containing the "Mobile Seal" Mark, must be accessible directly within the app.

V. DIRECT NOTICE AND PARENTAL CONSENT REQUIREMENTS

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

1. Participant must make reasonable efforts, taking into account available technology, to ensure that a parent receives direct notice of Participant's Online Information Practices with respect to Children, including notice of any material change in the Online Information Practices of Participant to which the parent has previously consented. With limited exceptions, Participant must provide direct notice to parents and obtain verifiable parental consent *before* collecting any PID from a Child. For exceptions to this requirement, see *Section V.D.* below.

2. Direct notice to parents sent to obtain prior verifiable parental consent must contain: (i) a hyperlink to Participant's Kids Privacy Statement (or that portion of Participant's General Privacy Statement that reflects its Online Information Practices with respect to Children) and notice that Participant has collected the parent's email address from the child in order to obtain consent; (ii) disclosure of the additional items of PID that Participant intends to collect from the Child, as well as potential opportunities for disclosure of the PID; (iii) disclosure that Participant must obtain the parent's permission to collect, use or disclose the PID collected from the Child; (iv) a description of the procedures by which a parent may give Participant such permission; and (v) notice that if the parent does not provide consent within a reasonable time, Participant will delete the parent's online contact information from its records.

B. Mechanisms for Obtaining Verifiable Parental Consent

Participant must take reasonable measures, in light of 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 Participant by mail, scan, or fax; (ii) requiring a parent to use a credit card in connection with a transaction on Participant's Monitored Product; (iii) having a parent call a toll-free telephone number staffed by trained personnel; (iv) having a parent connect to trained personnel via video-conference; (v) verifying the parent's identity by checking a form of

government-issued identification against databases of such information, provided that the identification information is deleted immediately after verification; (vi) using email accompanied by a PIN or password obtained by the parent through one of the verification methods described above; or (vii) using an approved vendor, such as Veratad Technologies.

C. Information Collected for Participant's Internal Use Only

Where Participant's use of PID is for internal purposes only, 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: (i) sending a delayed confirmatory email to the parent after receiving consent; or (ii) obtaining a postal address or telephone number from the parent, and confirming the parent's consent by letter or telephone call. If Participant implements such methods, the confirmation communication must include (a) all the information contained in the earlier email notice, and (b) instructions for how the parent can revoke the consent given in response to the earlier email.

D. Exceptions to Obtaining Prior Verifiable Parental Consent

Participant may collect a Child's name or email address prior to obtaining parental consent under the following exceptions:

1. **Obtaining Consent:** Participant may collect the name or email address of a parent or Child for the sole purpose of obtaining parental consent; provided, however, that if Participant does not obtain parental consent after a reasonable time from the initial date of collection, Participant shall permanently delete collected information from Participant's records. Participant must not use the collected name or email address to re-contact the parent or Child.

2. **One-Time Response:** Participant may collect an email address (or other online identifier) 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 re-contact the Child or for any other purpose and is subsequently deleted from Participant's records. Under this exception, Participant is not required to provide direct notice to a parent or to obtain verifiable parental consent.

3. **Multiple Responses:** Participant may collect the online contact information of a Child and parent only to respond directly, on more than one occasion, to a specific request from the Child, so long as such information is not used for any other purpose. In such instances, Participant must make reasonable efforts, taking into consideration available technology, to give direct notice to parents, which must: (i) include Participant's Kids Privacy Statement or that portion of Participant's General Privacy Statement that reflects its Online Information Practices with respect to Children; (ii) explain to the parent that Participant has collected the Child's email address 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 Participant 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, Participant may use the collected information for the purposes stated in the direct notice. This direct notice to parents must be sent immediately after Participant's initial response to the Child and before sending any additional responses.

4. **Protecting Child Safety:** Where Participant has used reasonable efforts to provide notice to the parent, Participant may collect a Child's name and email address only to the extent reasonably necessary to protect the safety of the Child on a Monitored Product, provided such information is used for the sole purpose of protecting the Child's safety and not used to re-contact the Child or for any other purpose, nor disclosed on the Monitored Products. In such cases, Participant must make reasonable efforts, taking into consideration available technology, to give direct notice to parents, which must: (i) include Participant's Kids Privacy Statement or that portion of Participant's General Privacy Statement that reflects its Online Information Practices with respect to Children; (ii) explain that Participant has collected the Child's name and email address to protect the Child's safety; (iii) explain that the parent may refuse to permit further contact with the Child and may require Participant 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, Participant may use the information for the purposes stated in the direct notice.

5. ***Protecting Others:*** Participant may collect a Child's name and email address only to protect the integrity or security of Participant's Monitored Products, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or pursuant to authorized investigations on matters related to public safety, provided such information is not used for any other purpose. Under this exception, Participant is not required to provide direct notice to parents.

VI. PROVIDING PARENTS ACCESS TO AND CONTROL OVER CHILDREN'S PERSONAL INFORMATION AND DATA

Participant must provide parents with the following information and opportunities to control use of their Child's PID:

- The specific information Participant has collected from the Child, including his/her name, address, telephone number, hobbies, etc.;
- An opportunity for the parent to prevent Participant from collecting or using PID about their Child in the future; and
- An opportunity for the parent to direct Participant to delete their Child's PID from Participant's records.

Participant must take reasonable measures, in light of available technology, to ensure that the person requesting access to or providing instructions about the Child's PID is the Child's parent. For acceptable verification mechanisms, refer to Section V.B. above.

VII. DATA COLLECTION AND SECURITY

A. Participant shall, upon ESRB's reasonable request, provide details regarding how PID is gathered from and/or tracked through Participant's Monitored Products, as well as disclosure regarding how such PID is utilized. If PID is not being utilized, Participant should not collect it.

B. Participant shall establish, implement and maintain reasonable procedures to protect the confidentiality, security and integrity of PID within its control, whether collected from adults or Children, from unauthorized access, use, alteration, distribution, or disclosure. Participant shall utilize appropriate, commercially reasonable methods (e.g., encryption) to protect any sensitive PID it collects, such as social security numbers or transactional information, including but not limited to financial information.

C. Participant must take reasonable steps to release Children's PID only to service providers and third parties capable of maintaining the confidentiality, security, and integrity of such information.

D. Participant shall take reasonable steps when collecting, creating, maintaining, using, distributing, or disclosing PID to assure that the data created, utilized and/or shared is up-to-date, complete and accurate.

E. Participant must implement reasonable and effective processes and/or mechanisms that allow users to correct material inaccuracies in PID, such as account or contact information. These processes and/or mechanisms must be easily comprehended and "user-friendly" and, once utilized, must confirm to users that the cited inaccuracies have been corrected.

F. If Participant's Monitored Products provide links to third-party web sites or apps, Participant should implement "exit messages" or "bumper pages" wherever users travel via such links to a third-party site or app to inform a user that: (i) he/she is leaving Participant's web site or app; and (ii) Participant's Terms of Use and Privacy Statement will no longer be applicable upon user's departure from Participant's website or app. Prior to implementation, Participant should submit the specific language it intends to utilize for this purpose to ESRB for approval.

EXHIBIT B

Proposed ESRB Privacy Certified Kids Seal Requirements

~~The following outlines the ESRB Privacy Certified Kids Seal Requirements ("Program Requirements") as referenced in the ESRB Privacy Certified Participation Agreement ("Agreement"). Any defined terms used in the Agreement shall have the same meaning when utilized here. If any of Participant's~~a Monitored ~~Web Sites or Mobile Apps are~~ Product is directed ~~at and/or collect Personally Identifiable Information from~~or targeted at children under the age of thirteen (13)~~, or if any section of Participant's Monitored Web Sites or Mobile Apps are directed at, targeted at, and/or collects Personally Identifiable Information from children under the age of thirteen (13), or if~~ *or* Participant has actual knowledge ~~that~~ it is collecting or maintaining ~~Personally Identifiable Information~~(or allowing a third party to collect or maintain) personal information or data from children under the age of thirteen (13) through ~~its~~a Monitored ~~Web Sites or Mobile Apps~~,Product, then Participant must comply with the ~~following~~ ESRB Privacy Certified ~~Kids~~Kids Seal Requirements. ~~If any of Participant's~~ set forth in this Schedule for all such Monitored ~~Web Sites or Mobile Apps are collecting information from citizens of the EU and~~Products, Participant has ~~enrolled in the EU Privacy Seal Program,~~submitted to ESRB for certification and on which Participant ~~must also comply with~~intends to display the Privacy Certified Kids Privacy seal and/or the ESRB Privacy Certified ~~EU Seal Requirements, , which shall, by reference, incorporate any and all applicable rules and definitions as outlined under the Children's Online Privacy Protection Act (as amended on December 19, 2012)~~Mobile seal.

I. DEFINITIONS

Child/Children means users resident in the United States ~~or Canada, or anywhere else in the world,~~ who are under thirteen (13) years of age.

Online Information Practices encompass, but are not limited to: (i) Participant's practices regarding consumer notification and consumer access to their ~~personal information;~~Personal Information and Data (as that term is defined below); (ii) Participant's practices with respect to the collection, use or disclosure of ~~personal information~~Personal Information and Data; (iii) Participant's practices regarding user choice and consent to how ~~personal information~~Personal Information and Data is used or shared; and (iv) security measures taken to protect ~~information~~Personal Information and Data provided by users.

~~**Personally Identifiable**~~ **Personal Information and Data ("PID")** means any information ~~that can be used~~ relating to ~~identify~~ an identified or identifiable individual ~~or which enables direct contact with an individual. This would include an individual's name,~~collected online ~~contact information (i.e. email addresses and screen names that function as email addresses~~, including, but not limited to:

- First and last name;
- Home or ~~reveal an individual's email~~other physical address~~), phone number, fax number, home address, social security number, driver's license number, credit card number, photos, videos, or~~

Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified
Formatted: Indent: First line: 1"
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Heading 1, Indent: First line: 0.25", Space Before: 12 pt, After: 3 pt
Formatted: Font: 12 pt, Not Bold
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt

~~audio containing the image or voice of a child, persistent identifiers (such as~~ or geolocation information;

- Online contact information (*e.g.*, email address, instant messenger identifier, video chat identifier, VOIP identifier, and screen name that permits direct contact with the individual online);
- Phone number;
- Persistent identifier (*e.g.*, a customer number held in a cookie ~~or a processor~~, internet protocol address, device serial number, ~~and~~or unique device identifier~~,~~), if additional PID is collected and/or the persistent identifier(s) are not used solely to support the internal operations of the Monitored Product;
- Photograph or video recording showing the individual's face or ~~IP address), or geolocation information sufficient to identify a street name and name of town.~~ otherwise containing PID in the photograph or recording or within the metadata of the photograph or recording;
- Audio recording capturing the individual's voice or otherwise containing PID within the recording or the metadata of the recording, except to the extent such audio recordings are used solely to effectuate speech-to-text functionality in the Monitored Product and deleted immediately thereafter; and
- Social security number or other government identification number.

Demographic information ~~that is combined with personal information~~ (including, but not limited to, gender, age, date of birth, educational background, or political affiliation) also becomes ~~Personally Identifiable Information. Personally Identifiable Information~~PID when combined with other information enabling the individual to be identified. PID does not include information that is ~~encoded or~~ rendered anonymous~~, or publicly available information that has not been combined with non-public Personally Identifiable Information~~.

Privacy Statement means the statement, posted on the Monitored ~~Web Sites or Mobile Apps~~Products, which discloses Participant's up-to-date policies regarding user privacy and Participant's practices with respect to the collection, use and disclosure of ~~Personally Identifiable Information, as such practices may be updated from time to time~~PID.

~~**Privacy Risk Assessment** means the initial, pre-certification report provided by ESRB to a company before it becomes a Participant in the Program, which reflects ESRB's assessment of the legal and business risks posed by the company's then-current Privacy Statement, data gathering practices and online privacy disclosures.~~

II. PROGRAM DOCUMENTS AND PROCEDURES

C. ~~A.~~ Initial ~~SAQ/Certification~~Compliance Report

~~If it has not already done so during the pre-certification phase in anticipation of receipt of ESRB's Privacy Risk Assessment, Participant shall fully complete a Self Assessment Questionnaire ("SAQ") and return it to ESRB. In providing the completed SAQ, Participant understands that ESRB may rely on the statements contained therein for the purpose of determining~~

Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified, Indent: First line: 0.25"
Formatted: Justified
Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 1"
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt

Participant's information collection practices as well as Participant's overall qualification for the ESRB Privacy Certified Program. An authorized representative of Participant shall sign and attest that the information provided in the SAQ is true and accurate as of the date submitted.

ESRB shall review the completed SAQ, along with Participant's Privacy Statement and related information collection practices, andOnline Information Practices with respect to the Monitored Products. ESRB shall assess the state of Participant's overall compliance with the Program Requirements. Upon completing this review, ESRB will after which it shall provide Participant with(i) required and suggested changes to Participant's Privacy Statement; and (ii) a comprehensive report detailing any and all required and suggested changes to Participant's Privacy Statement and/orOnline Information Practices with respect to the Monitored Web Sites or Mobile Apps ("CertificationProducts ("Compliance Report").

Participant mustshall implement all changes required to the Privacy Statements and by the CertificationCompliance Report and attest to ESRB that it has done so by returning a signed copy of the Certification Report. ESRB will in writing. ESRB shall then complete a final review of the Privacy Statement and Monitored Web Sites or Mobile Apps and, ifProducts. If all the required changes have been implemented, or otherwise resolved, ESRB shall provide Participant with written approval to use and access to the appropriate Program Marks.

B. Onsite Compliance Reviews

1. At the time Participant is certified to enter the Program, Participant shall be subject to an onsite compliance review by ESRB. The onsite review shall be scheduled in advance for a mutually-convenient time and shall be conducted during Participant's normal business hours. Participant shall bear the reasonable costs (e.g., travel, lodging, meals) associated with this review and agrees to reimburse ESRB within thirty (30) days of receipt of an invoice detailing these charges.

2. Should Participant's compliance record or ongoing concerns with respect to the Monitored Web Sites or Mobile Apps so warrant, ESRB may conduct additional onsite reviews, the necessity of which shall be determined by ESRB in its sole discretion. Participant shall reimburse ESRB for the reasonable costs associated with any such onsite review; provided, however, that such reviews shall be limited to no more than one per calendar year.

3. Participant may also request additional onsite visits by ESRB (e.g., for staff training or educational purposes), the reasonable costs of which shall be borne by Participant.

C. Biannual Monitoring and Compliance Reports

Twice a yearAt least once during the Initial Term and no more than twice during each Renewal Term ("Reporting Periods") during the Term of the Agreement,"), ESRB shall provide Participant with a report ("Compliance Report") that will: (i) list all of the Monitored Web Sites or Mobile Apps as well as any new sites that have come to ESRB's attention during that Reporting PeriodProducts; (ii) describe changes to Participant's Privacy Statement and/or Monitored Web

Formatted: Font: +Body (Calibri), 12 pt (×19)
Formatted: Justified, Indent: First line: 1"
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Indent: First line: 0.5"
Formatted: Indent: Left: 0"
Formatted: Font: +Body (Calibri), 12 pt (×5)

~~Sites or Mobile Apps which~~ Products that are necessary for Participant to remain compliant with the ~~Program~~Kids Seal Requirements; and (iii) propose changes which, although not required under the ~~Program~~Kids Seal Requirements, reflect "best practices" ~~which~~that are highly recommended by ESRB. Within three (3) weeks of Participant's receipt of a Compliance Report, Participant must notify ESRB, through ESRB's SharePoint system (or through whatever other means may be specified by ESRB pursuant to its then-current policy), that Participant has implemented all changes required by the Compliance Report. If Participant needs more than three weeks to implement the required changes, Participant shall notify ESRB immediately and provide a time frame within which it commits to complete all changes.

~~In order for~~ For ESRB to provide thorough and accurate Compliance Reports, Participant must provide ESRB full access to the Monitored ~~Web Sites or Mobile Apps~~Products, including access to "members only" or password-protected areas of the Monitored ~~Web Sites or Mobile Apps~~Products.

III. CONTINUING OBLIGATIONS OF PARTICIPANT

A. Designation of Site Coordinator

~~At the time the Agreement is executed,~~ Participant shall name a coordinator for the Monitored ~~Web Sites or Mobile Apps~~Products ("Site Coordinator") who shall be ESRB's primary contact, ~~and,~~ Participant shall ~~keep~~notify ESRB ~~apprised should it designate~~in the event of a ~~different~~ change to the individual ~~to act~~designated as Site Coordinator. The Site Coordinator shall be ~~the employee~~ responsible for the effectuation and implementation of ~~the~~Participant's Online Information Practices reflected in its Privacy Statement and compliance with ~~these Program~~the Kids Seal Requirements. All notices from ESRB shall be directed to the Site Coordinator.

B. Notifying ESRB of Material Changes

~~4.~~ 1. Participant ~~is required to~~shall notify ESRB in advance of any material change(s) to its Online Information Practices, including, by way of example, changes to Participant's Terms of Use or End User License Agreement; changes to its data security infrastructure; or the roll-out of any new sweepstakes, contest or similar promotion ~~on a~~through the Monitored ~~Web Site or Mobile App.~~ Products.

~~5.~~ 2. Participant ~~must~~shall obtain prior approval from ESRB for ~~any~~

Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified, Indent: First line: 1"
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified, Indent: Left: 0.5"
Formatted: Justified, Indent: First line: 0.25"
Formatted: Justified
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified, Indent: First line: 1"
Formatted: Indent: First line: 1", No bullets or numbering
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified, Indent: First line: 1"
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Indent: Left: 0", First line: 1"
Formatted: Indent: First line: 1", No bullets or numbering
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt

all substantive modification to its Privacy Statement, whether such modification results from a material change in Participant's Online Information Practices, the revamping of a Monitored ~~Web Site or Mobile App~~Products, or otherwise.

~~6.~~ 3. Where changes to Participant's Monitored ~~Web Sites or Mobile Apps~~Products, Privacy Statement or Online ~~Privacy~~Information Practices have been implemented, Participant may be required to submit ~~an updated~~ Self-Assessment Questionnaire ("SAQ") or provide updated information in a form determined by ESRB. Participant may also be required to submit a ~~new~~ SAQ if Participant has undergone a "change in control," ~~as defined in Section 2.5 of the Agreement~~, or if there has been an investigation of Participant's practices by a federal or state authority, agency or regulatory body or any unit of federal or state government.

C. Notifying Users of Material Changes

Participant ~~is required to~~shall notify users of any material change(s) in its Online Information Practices or Privacy Statement. Notice should be provided to users prior to the change taking effect. ~~Participant shall give ESRB advance notice of any material change so that ESRB may ensure that users are properly notified.~~ Different types of material changes may require different forms of notice to users. If, while reviewing Participant's Monitored ~~Web Sites~~Products in the normal course, ESRB discovers a material change of which it was not previously notified, ESRB will advise Participant ~~in the next scheduled Compliance Report~~ of the type of notice Participant must provide to users of the Monitored ~~Web Sites or Mobile Apps.~~ Products.

~~D.~~

D. Resolution of Consumer Complaints

1. Participant ~~must~~shall implement procedures to receive, investigate and resolve privacy inquiries and complaints from users. Where Participant's internal mechanisms are unable to address a user grievance effectively, Participant shall refer the user to ESRB for~~and advise the user of ESRB's D~~dispute R~~resolution process.~~

2. ESRB shall ~~maintain a consumer online hotline~~provide contact information on its website, which visitors to Participant's Monitored ~~Web Sites or Mobile Apps~~Products may use to contact ESRB with inquiries or complaints regarding ~~these sites.~~a Monitored Product. After determining the nature of the complaint, ESRB shall respond in one of the following ways.

Formatted ... [1]
Formatted: Justified, Indent: First line: 1"
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified, Indent: Left: 0", First line: 1"
Formatted: Indent: First line: 1", No bullets or numbering
Formatted ... [2]
Formatted ... [3]
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified, Indent: First line: 1"
Formatted: Justified, Indent: Left: 0", First line: 1"
Formatted: Justified
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified, Indent: First line: 1"
Formatted ... [4]
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, ... + Start at: 4 + Alignment: Left + Aligned at: 0.5" + Indent at: 1"
Formatted ... [5]
Formatted: Justified, Indent: First line: 1"
Formatted ... [6]
Formatted ... [7]
Formatted ... [8]

d. If the question, concern or complaint is not privacy-related, ESRB shall either forward ~~the email~~it to the individual at Participant's company designated for such purpose. ~~or~~ redirect the consumer to the appropriate contact mechanism (e.g., support page).

e. If the ~~consumer's email~~inquiry or complaint is privacy-related and presents a question or an issue ESRB can independently address, ESRB shall respond directly to the consumer. ~~If analysis and/or resolution of the consumer's complaint requires input from Participant, ESRB shall contact Participant to obtain the necessary information. Participant shall cooperate with ESRB in resolving consumer complaints.~~

f. If inquiry or complaint is privacy related, but requires information or input from Participant, ESRB shall contact Participant. Participant shall cooperate with ESRB in resolving consumer complaints.

3. If neither Participant nor ESRB succeeds in independently resolving a consumer grievance, and the consumer wishes to pursue the matter further, Participant agrees to fully participate, along with the consumer, in a~~ESRB's D~~dispute R~~r~~esolution process conducted by ESRB and agrees to accept ESRB's judgment as final.

E. Required Notice to ESRB

Participant shall notify ESRB in writing within thirty (30) days if Participant: (i) changes its name; (ii) undergoes a "change in control," ~~as defined in Section 2.5 of the Agreement~~; or (iii) changes the domain name of any Monitored ~~Web Site or Mobile App~~Product.

IV. PRIVACY STATEMENT

A. Content of General Privacy Statement

Participant shall maintain and abide by a Privacy Statement that is either written by Participant and approved by ESRB, in its sole discretion, or written by ESRB. The Privacy Statement shall clearly set forth Participant's Online Information Practices. The Privacy Statement must link only to and from web pages that are in the English language. If a Participant wishes to link the Privacy Statement to or from a web page or mobile application in a language other than English, the Privacy Statement must be translated and localized for the applicable language/locality. At a minimum, Participant's posted Privacy Statement shall provide disclosure

Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: List Paragraph, Justified, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 1" + Indent at: 1.5"
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified, Indent: First line: 1"
Formatted: Justified, Indent: First line: 1"
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified
Formatted: Justified, Indent: First line: 1"
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt

to users with respect to each of the following elements:

~~notice~~

- 1. Notice that the ~~site is a participant in~~ Monitored Product has been reviewed and certified by the ESRB Privacy Certified Program;
- 2. ~~a~~A full description of how users ~~of the site~~ can contact Participant, including the Participant's name, postal address, and email address;
- ~~1.~~ ~~a~~A full description of how users can ~~of the site can~~ contact ESRB with questions or concerns about Participant's Privacy Statement or ~~privacy practices;~~
- 3. ~~a description of the Personally Identifiable~~Online Information ~~that is~~ Practices;
- 4. A complete list of all PID collected through the ~~site~~Monitored Product, how each PID identified is collected, and how it is used;
- 5. ~~the~~The identity (including name, address and e-mail address) of all ~~of the organizations~~entities ~~(i.e., third parties)~~ that are collecting ~~Personally Identifiable Information~~or maintaining PID on behalf of or through the ~~site~~Monitored Product;
- ~~2.~~ ~~the manner in which Personally Identifiable Information collected through the site will be used;~~
- 6. ~~the~~The entities (if any) with whom ~~Personally Identifiable Information~~PID collected through the ~~site~~Monitored Product is shared, ~~and the entities that collect~~ or ~~maintain~~ disclosed, including the types of businesses in which any third parties are engaged, the general purpose for which the information ~~on behalf of~~ is used by the third parties, whether the ~~site or app~~third parties have agreed to maintain the confidentiality, security, and integrity of the PID collected by Participant;
- 7. ~~notice~~Notice of whether Participant supplements ~~Personally Identifiable Information~~PID collected ~~on~~through the ~~site~~Monitored Products with information from other sources and, if so, a description of the PID and the sources from which they were collected;
- 8. ~~disclosure~~Disclosure of the tracking technologies, if any, used on the ~~site~~Monitored Product either by Participant or by an authorized third party;
- 9. ~~an~~An explanation of when and how users may exercise opt-in and/or opt-out options, including the choices available to them regarding how their PID is collected and used;
- 10. ~~the~~The nature of the security measures in place on the ~~site~~Monitored Product;
- 11. ~~notice that Personally Identifiable Information~~Notice that PID provided to Participant may be subject to disclosure in response to judicial or other government subpoenas, warrants, or orders;
- 12. ~~notice~~Notice that information posted by users in online bulletin boards, chat rooms, news groups, or other public forums may be displayed publicly;

Formatted: Font: +Body (Calibri), 12 pt
Formatted ... [9]
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted ... [10]
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted ... [11]
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted ... [12]
Formatted ... [13]
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt

•13. ~~the~~The notification procedures to be utilized by Participant in the event of a material change in its Online Information Practices and/or Privacy Statement; and

•14. ~~disclosure~~Disclosure of the effective date or last date on which the Privacy Statement was updated (i.e., "updated as of").

B. Content of Kids Privacy Statement

If Participant is collecting ~~Personally Identifiable Information~~PID from Children, or if any portion of Participant's Monitored ~~Web Sites or Mobile Apps~~Products are directed to or target Children, then Participant either must implement a separate Kids Privacy Statement, or incorporate into its General Privacy Statement a section specifically devoted to Participant's Online Information Practices with respect to Children.

In addition to the elements set forth in Section IV.A. above, Participant's Kids Privacy Statement, or, if there is no separate Kids Statement, that portion of Participant's General Privacy Statement reflecting its Online Information Practices with respect to Children, must contain the following elements:

•1. Disclosure of the manner in which Children's ~~Personally Identifiable Information~~PID is collected through the ~~site or app~~Monitored Product and how it will be used, ~~including but not limited~~ (*e.g.*, to ~~use for purposes of fulfilling~~fulfill a requested transaction, for record keeping purposes, ~~or~~ for the purpose of marketing products or services to ~~the Child; Children~~, etc.);

•2. Notice that a Child's participation in a chat room, bulletin board, or other online forum provided by Participant may result in such Child's public disclosure of ~~Personally Identifiable Information~~PID, and notice of Participant's policy to remove any such ~~Personally Identifiable Information~~PID if and when discovered;

~~3.~~

3. Notice that a parent has the option to consent to Participant's collection and use of their Child's ~~Personally Identifiable Information~~PID without consenting to Participant's disclosure of that information to third parties;

4. A description of the procedures pursuant to which parents can prevent Participant's disclosure of their Child's ~~Personally Identifiable Information~~PID to third parties;

5. Disclosure that Participant may not condition a Child's participation in an activity on such ~~Child~~Child's disclosing more ~~Personally Identifiable Information~~PID than is reasonably necessary to participate in such activity;

~~9.~~ 6. Notice that parents may ~~view and elect to remove their Child's Personally Identifiable Information and may also~~ refuse to allow Participant ~~to~~ and/or any third party from further ~~collect~~collecting or ~~use~~using their Child's ~~Personally Identifiable Information; and~~ PID;

~~10.~~ 7. A description of the process by which a parent can, for any purpose, access ~~and view~~, correct, or delete their Child's ~~Personally Identifiable~~PID; ~~Information~~

8. A description of the process by which third parties give parents access to review, correct, or delete their Child's PID, including for the purpose of preventing disclosure to third parties of their Child's ~~Personally Identifiable Information.~~ PID.

E. C. Placement of Kids Privacy Statement and Other ESRB Marks

Participant must provide, on its home page and on any pages where ~~Personally Identifiable Information~~PID is collected from Children, a prominent and clearly labeled link to its ~~Kids~~ Privacy Statement ~~or to that portion of its General Privacy Statement that reflects Participant's Online Information Practices with respect to Children.~~ If the Monitored Product is a website, Participant should ~~label this link with~~post the "~~Kids~~Kids Privacy Seal" Mark ~~identified on Schedule D. If it is not possible to use this Mark in a given location, ESRB may, in the exercise of its discretion, permit use of hyperlink text with the phrase "Kids~~near the link to the Privacy Statement. The Kids Privacy ~~Policy" or its approved equivalent. The Kids~~ Seal Mark must link directly to Participant's ~~Kids~~membership confirmation page hosted at esrb.org.

If the Monitored Product is an online app, a link to the Privacy Statement ~~or the portion of Participant's~~must be in the app store, available prior to download. A Privacy Statement ~~describing Participant's Online Information Practices with respect to Children. Participant must provide, at the top and/or bottom of Participant's Kids Privacy Statement, a clearly labeled link to Participant's General Privacy Statement~~, preferably a short form template containing the "Mobile Seal" Mark, must be accessible directly within the app.

V. DIRECT NOTICE AND PARENTAL CONSENT REQUIREMENTS

Formatted ... [14]
Formatted ... [15]
Formatted ... [17]
Formatted ... [16]
Formatted ... [18]
Formatted ... [19]
Formatted ... [21]
Formatted ... [20]
Formatted ... [22]
Formatted ... [23]
Formatted ... [24]
Formatted ... [25]
Formatted ... [26]
Formatted ... [27]
Formatted ... [28]
Formatted ... [29]
Formatted ... [30]
Formatted ... [31]
Formatted ... [32]
Formatted ... [33]
Formatted ... [34]
Formatted ... [35]
Formatted ... [36]
Formatted ... [37]
Formatted ... [38]
Formatted ... [39]
Formatted ... [40]
Formatted ... [41]
Formatted ... [42]
Formatted ... [43]
Formatted ... [44]
Formatted ... [45]
Formatted ... [46]
Formatted ... [47]
Formatted ... [48]
Formatted ... [49]
Formatted ... [50]
Formatted ... [51]
Formatted ... [52]
Formatted ... [53]
Formatted ... [54]
Formatted ... [55]
Formatted ... [56]
Formatted ... [57]
Formatted ... [58]
Formatted ... [59]
Formatted ... [60]

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

1. Participant must make reasonable efforts, taking into account available technology, to ensure that a parent receives direct notice of Participant's Online Information Practices with respect to Children, including notice of any material change in the Online Information Practices of Participant to which the parent has previously consented. With limited exceptions, Participant must provide direct notice to parents and obtain verifiable parental consent *before* collecting any ~~Personally Identifiable Information~~PID from a Child. For exceptions to this requirement, see *Section V.D.* below.

2. Direct notice to parents sent to obtain prior verifiable parental consent must contain: (i) a hyperlink to Participant's Kids Privacy Statement (or that portion of Participant's General Privacy Statement that reflects its Online Information Practices with respect to Children) and notice that Participant has collected the parent's address from the child in order to obtain consent; (ii) disclosure of the additional items of ~~Personally Identifiable Information~~PID that ~~the~~ Participant intends to collect from the Child, as well as potential opportunities for disclosure of the PID; (iii) disclosure that Participant must obtain the parent's permission to collect ~~and~~, use ~~the Personally Identifiable Information~~or disclose the PID collected from the Child; (iv) a description of the procedures by which a parent may give Participant such permission; and (v) notice that if the parent does not provide consent within a reasonable time, Participant will delete the parent's online contact information from its records.

B. Mechanisms for Obtaining Verifiable Parental Consent

Participant must take reasonable measures, in light of 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 Participant by mail, scan, or fax; (ii) requiring a parent to use a credit card in connection with a transaction on Participant's ~~site~~Monitored Product; (iii) having a parent call a toll-free telephone number staffed by trained personnel; (iv) having a parent connect to trained personnel via video-conference; (v) verifying the parent's identity by checking a form of government-issued identification against databases of such information, provided that the identification information is deleted immediately after verification; ~~or~~ (vi) using e-mail accompanied by a PIN or password obtained by the parent through one of the verification methods described above; or (vii) using an approved vendor, such as Veratad Technologies.

C. Information Collected for Participant's Internal Use Only

Where Participant's use of ~~Personally Identifiable Information~~PID is for internal purposes only, 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: (i) sending a delayed confirmatory email to the parent after receiving consent; or (ii) obtaining a postal address or telephone number from the parent, and confirming the parent's

Formatted: Justified
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt, Not Italic
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt

consent by letter or telephone call. If Participant implements such methods, ~~Participant must provide notice in the~~ the confirmation communication ~~that the~~ must include (a) all the information contained in the earlier email notice, and (b) instructions for how the parent can revoke ~~any~~the consent given in response to the earlier email~~, coupled with instructions on how to revoke such consent~~.

Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt

D. Exceptions to Obtaining Prior Verifiable Parental Consent

Participant may collect a Child's name or email address prior to obtaining parental consent under the following exceptions:

1. **Obtaining Consent:** Participant may collect the name or email address of a parent or ~~child~~Child for the sole purpose of obtaining parental consent; provided, however, that if Participant does not obtain parental consent after a reasonable time from the initial date of collection, Participant shall permanently delete collected information from Participant's records. Participant must not use the collected name or email address to re-contact the parent or Child.

Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt

2. **One-Time Response:** Participant may collect an email address (or other online identifier) from a ~~child~~Child for the sole purpose of responding directly, on a one-time basis, to a specific request from the ~~child~~Child -- so long as such information is not used to re-contact the ~~child~~Child or for any other purpose and is subsequently deleted from Participant's records. Under this exception, Participant is not required to provide direct notice to a parent or to obtain verifiable parental consent.

Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt

3. **Multiple Responses:** Participant may collect the online contact information of a Child and parent ~~in order~~only to respond directly, on more than one occasion, to a specific request from the Child, so long as such information is not used for any other purpose. In such instances, Participant must make reasonable efforts, taking into consideration available technology, to give direct notice to parents, which must: (i) include Participant's Kids Privacy Statement or that portion of Participant's General Privacy Statement that reflects its Online Information Practices with respect to Children; (ii) explain to the parent that Participant has collected the Child's email address 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 Participant 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, Participant may use the collected information for the purposes stated in the direct notice. This direct notice to parents must be sent immediately after Participant's initial response to the Child and before sending any additional responses.

Formatted: Font: +Body (Calibri), 12 pt

4. **Protecting Child Safety:** Where Participant has used reasonable efforts to provide notice to the parent, Participant may collect a Child's name and email address

only to the extent reasonably necessary to protect the safety of the Child on a Monitored ~~Web Site or Mobile App~~Product, provided such information is used for the sole purpose of protecting the Child's safety and not used to re-contact the Child or for any other purpose, nor disclosed on the Monitored ~~Web Sites or Mobile Apps.~~Products. In such cases, Participant must make reasonable efforts, taking into consideration available technology, to give direct notice to parents, which must: (i) include Participant's Kids Privacy Statement or that portion of Participant's General Privacy Statement that reflects its Online Information Practices with respect to Children; (ii) explain that Participant has collected the Child's name and email address to protect the Child's safety; (iii) explain that the parent may refuse to permit further contact with the Child and may require Participant 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, Participant may use the information for the purposes stated in the direct notice.

5. **Protecting Others:** Participant may collect a Child's name and email address only to protect the integrity or security of Participant's Monitored ~~Web Sites or Mobile Apps~~Products, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or pursuant to authorized investigations on matters related to public safety, provided such information is not used for any other purpose. Under this exception, Participant is not required to provide direct notice to parents.

VI. PROVIDING PARENTS ACCESS TO AND CONTROL OVER CHILDREN'S ~~PERSONALLY IDENTIFIABLE~~PERSONAL INFORMATION AND DATA

Participant must provide parents with the following information and opportunities to control use of their Child's ~~Personally Identifiable Information~~PID:

- ~~the~~The specific information Participant has collected from the Child, including his/her name, address, telephone number, hobbies, etc.;
- ~~an~~An opportunity for the parent to prevent Participant from collecting or using ~~Personally Identifiable Information~~PID about their ~~child~~Child in the future; and
- ~~an~~An opportunity for the parent to direct Participant to delete their Child's ~~Personally Identifiable Information~~PID from Participant's records.

Participant must take reasonable measures, in light of available technology, to ensure that the person requesting access to or providing instructions about the Child's ~~Personally Identifiable Information~~PID is the Child's parent. For acceptable verification mechanisms, refer to Section V.B. above.

Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt, Not Italic
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified, Indent: Hanging: 0.25"
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified, Bulleted + Level: 1 + Aligned at: 0.5" + Tab after: 0.75" + Indent at: 0.75"
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt

VII. DATA COLLECTION AND SECURITY

A. Participant shall, upon ESRB's reasonable request, provide details regarding how ~~Personally Identifiable Information~~PID is gathered from and/or tracked through Participant's Monitored ~~Web Sites or Mobile Apps~~Products, as well as disclosure regarding how such ~~Personally Identifiable Information~~PID is utilized. If PID is not being utilized, Participant should not collect it.

B. ~~B.~~ Participant ~~must~~shall establish, implement and maintain reasonable procedures to protect the confidentiality, security and integrity of ~~Personally Identifiable Information~~PID within its control, whether collected from adults or ~~children~~Children, from unauthorized access, use, alteration, distribution, or disclosure. Participant shall utilize appropriate, commercially reasonable methods (e.g., encryption) to protect any sensitive ~~information~~PID it collects, such as social security numbers or transactional information, including but not limited to financial information.

C. ~~.~~Participant must ~~also~~ take reasonable steps to release ~~children's personally identifiable information~~Children's PID only to service providers and third parties that are capable of maintaining the confidentiality, security, and integrity of such information.

~~C~~D. Participant shall take reasonable steps when collecting, creating, maintaining, using, distributing, or disclosing ~~Personally Identifiable Information~~PID to assure that the data created, utilized and/or shared is up-to-date, complete and accurate.

~~D~~E. Participant must implement reasonable and effective processes and/or mechanisms ~~which~~that allow users to correct material inaccuracies in ~~Personally Identifiable Information~~PID, such as account or contact information. These processes and/or mechanisms must be easily comprehended and "user-friendly" and, once utilized, must confirm to users that the cited inaccuracies have been corrected.

~~E~~F. If Participant's Monitored ~~Web Sites or Mobile Apps~~Products provide links to third-party web sites or apps, Participant ~~must~~should implement "exit messages" or "bumper pages" wherever users travel via such links to a third-party site or app to inform a user that: (i) he/she is leaving Participant's web site or app; and (ii) Participant's Terms of Use and Privacy Statement will no longer be applicable upon user's departure from Participant's web site or app. Prior to implementation, Participant ~~must~~should submit the specific language it intends to utilize for this purpose to ESRB for approval.

Formatted: Indent: First line: 0.25"
Formatted: Justified
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 2 + Alignment: Left + Aligned at: 0.5" + Indent at: 1"
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Indent: First line: 0.5"
Formatted: Justified
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Font: +Body (Calibri), 12 pt
Formatted: Justified, Indent: First line: 0.5"