United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

August 13, 2018

John M. Falzone, Esq.
Vice President, ESRB Privacy Certified
Entertainment Software Rating Board
420 Lexington Avenue
Suite 2240
New York, New York 10170

Re: Application of the Entertainment Software Rating Board for Approval of Modifications to its Children's Online Privacy Protection Rule[1] Safe Harbor Program

Dear Mr. Falzone:

This letter is to inform you that the Federal Trade Commission ("FTC" or "Commission") has approved the Entertainment Software Rating Board's ("ESRB" or the "Company") application to modify its Commission-approved Children's Online Privacy Protection Act ("COPPA")[2] safe harbor program.

The Commission approved ESRB's original COPPA safe harbor program in 2001, modifications in 2005, and its revised program, to comply with the 2012 amendments to the COPPA Rule, in 2013. ESRB submitted this application to modify its existing safe harbor program ("ESRB Modified Program") on March 13, 2018. The Commission announced ESRB's request to modify its safe harbor program on April 5, 2018, and received public comment on the application through May 9, 2018.

The ESRB Modified Program makes several substantive changes that ESRB indicates are intended to better align the program with the Commission's COPPA-related regulations and guidance, and to allow the ESRB to monitor clients to ensure they remain in compliance with the law. For example, the Modified Program updates the definition of "Personal Information and Data," adds text to make it clear that members shall not collect information and data that they are not utilizing, and clarifies that links to privacy statements must be clear and prominent.

[1] 16 C.F.R. Part 312.
[2] 15 U.S.C. §§ 6501-6506.

The Commission received five comments in response to its request for comment on ESRB's application, three of which were germane.[3] An individual, Ms. Aguirre, recommended that the FTC review COPPA and other programs, such as the Safe Harbor Program, on an annual basis. We agree that this type of review is important. The Commission does conduct an annual review of its approved Safe Harbor programs, as provided by the Rule.[4] With respect to ESRB's proposed changes, the commenter recommended that ESRB clarify that links to privacy statements be prominent and clearly labeled. This concern, also, is addressed in the Rule. Section 312.4(d) requires, among other things, that an "operator must post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page or screen of its Web site or online service, *and*, at each area of the Web site or online service where personal information is collected from children."[5] Furthermore, '"clear and prominent' means that the link must stand out and be noticeable to the site's visitors through use, for example, of a larger font size in a different color on a contrasting background. The Commission does not consider 'clear and prominent' a link that is in small print at the bottom of the home page, or a link that is indistinguishable from a number of other, adjacent links."'[6] ESRB's program does in fact require the link to be clear and prominent.

The Campaign for a Commercial-Free Childhood ("CCFC") and the Center for Digital Democracy ("CDD") filed a joint comment through their counsel, the Institute for Public Representation. CCFC and CDD recommended that absent changes, the FTC should reject ESRB's application to modify its safe harbor program because in their view, ESRB's proposed modification would reduce protections for children below the bar set by COPPA. The organizations recommended a number of amendments to ESRB's application including: (1) replacing language regarding the number of compliance reports required; (2) adding language explaining how ESRB will collect information about a participant's "Online Information Practices;" (3) revising the proposed exceptions for speech-to-text recordings and persistent identifiers within the definition of Personal Information and Data ("PID"); (4) defining the term "Monitored Products"; (5) retaining language from the existing program that defines street-level geolocation information as PID, which ESRB had proposed to remove; (6) replacing "photograph or video recording showing an individual's face" in the definition of PID with "Photograph or video that contains the individual's image"; (7) reinstating the language requiring each member to link to its privacy statement; and (8) replacing the word "should" with "must" or "shall" in the sentence, "If PID is not being utilized, Participant should not collect it." The Commission agrees that these proposed amendments would help ensure that ESRB's Modified Program is compliant with COPPA, and the program as approved reflects these modifications.

Another comment came from the Electronic Privacy Information Center ("EPIC"). While EPIC commended ESRB on some of its proposed changes, the organization expressed concern that other proposed modifications would diminish privacy safeguards and fall below

---

[3] These comments are available at https://www.ftc.gov/policy/public-comments/2018/05/initiative-749. Two individuals' comments were not related to ESRB's safe harbor program or modifications.
[4] 16 C.F.R. Section 312.11(d).
[5] 16 C.F.R. Section 312.4(d) (italics in original).
[6] 1999 Statement of Basis and Purpose, 64 Fed. Reg. 59888, 59894.

COPPA's requirements.[7] One modification EPIC encouraged the Commission to reject was ESRB's proposal to narrow the definition of "Child/Children" to only residents in the United States. The Commission agrees with EPIC's comment. As COPPA's protections are not limited only to U.S. residents, the definition of "child" in the ESRB program has been revised to remove the limitation and to reflect the definition of "child" as stated in the Rule.

EPIC also took issue with ESRB's request to terminate the "Initial Self-Assessment Questionnaire."[8] While we see the value in a self-assessment questionnaire, ESRB's program demonstrates that ESRB plans to obtain the same information through other means, including through direct questions from the ESRB. We see no reason to mandate that the information be collected initially by the member alone so long as the ESRB obtains a comprehensive understanding of members' information practices at the end of the process.

Further, EPIC disagreed with ESRB's proposed changes to the definition of PID with respect to information "rendered anonymous" and "collected online." ESRB's reference to "anonymous" data could be read as suggesting that member companies may collect personal information, such as email address and phone number, without notice and consent as long as they then de-identify it; generally, however, companies must provide notice and obtain verifiable parental consent if personal information is collected, even if it is later anonymized.[9] Accordingly, the Commission agrees with EPIC's comment and has rejected this change. As to the proposed change related to information "collected online," COPPA's definition of personal information applies to "individually identifiable information about an individual collected online…."[10] Thus, the Commission believes ESRB's change is consistent with the Rule.

Finally, EPIC encouraged the Commission to reject ESRB's proposed modification to make use of "exit messages" or "bumper pages" a best practice rather than a requirement. "Exit messages" or "bumper pages" are pop-ups or separate screens used to notify users that they are leaving one website or app and entering another. These notifications are useful in helping operators distinguish their website or app from another website or app's. Essentially, "exit messages" or "bumper pages" notify users that an operator's terms of use or privacy policy is inapplicable once the user clicks on the link to the other website or app. The Commission notes

---

[7] EPIC also recommended that COPPA "establish a general understanding that the collection and use of information on young children should be treated with care and avoided if possible." Comment of EPIC, at 9. The COPPA Rule already requires data minimization. 16 C.F.R. § 312.10. EPIC also recommended, without elaboration, that the definition of "disclosure" be strengthened "to address the opaque manner in which social networking sites like Facebook share information with third parties." Comment of EPIC, at 5-6. It is unclear how this comment relates to the underlying issue of whether ESRB's proposed modifications meet the standard for approval. Furthermore, "disclosure" is not a defined term in ESRB's application.

[8] Comment of EPIC at 7. EPIC also objected to the proposed removal of the definition of "Privacy Risk Assessment." Although that term was defined, the term was not employed in ESRB's program, so removing the definition does not affect the program. We believe the other elements of ESRB's program satisfy the Rule's elements.

[9] A company may, however, operate a moderated chat room, reviewing and filtering personal information from the chat before posting.

[10] 16 C.F.R. § 312.2 (definition of "personal information"). EPIC raised the issue of offline collection in the particular context of Radio Frequency Identification ("RFID"). By agreeing to ESRB's limitation of its program to online collection, the Commission is not taking the position that collection of information via RFID is necessarily offline, as some RFID use cases involve transmission of RFID data via TCP/IP.

that the COPPA Rule does not require that operators use "exit messages" or "bumper pages." We agree that such measures are best practices.

For Commission approval, self-regulatory guidelines must include: (1) a requirement that participants in the safe harbor program implement substantially similar requirements that provide the same or greater protections for children as those contained in the Rule; (2) an effective mandatory mechanism for the independent assessment of the safe harbor program participants' compliance with the guidelines; and (3) disciplinary actions for noncompliance by safe harbor participants.[11] As noted above, two of the comments opposed approval of the Modified Program without modification, however, ESRB made all of the changes requested by CCFC and CDD, and made many of the changes requested by EPIC.

For the reasons stated above, the Commission has determined that the ESRB Modified Program, as modified after public comment as attached, satisfies the Rule criteria, and, therefore, approves your request.

By direction of the Commission.

Donald S. Clark
Secretary

[11] 16 C.F.R. § 312.11(b).

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 an individual under the age of 13.

Monitored Products include any and all websites, mobile applications, online services, and internet-connected devices, which are operated by Participant and which Participant has submitted to ESRB for certification and monitoring in accordance with the ESRB Privacy Certified Kids Seal Requirements.

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 sufficient to identify street name and name of a city or town;
- 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;
- A persistent identifier that can be used to recognize an individual over time and across different websites or online services (*e.g.*, a customer number held in a cookie, internet protocol address, device serial number, or unique device identifier);
- Photograph or video recording that contains the image, voice or any other PID of a child, including 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; 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.

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 obtain relevant information from Participant about its Online Information Practices with respect to the Monitored Products. ESRB shall gather relevant information about Participant's Online Information Practices utilizing one or more of a variety of methods, which include (i) requesting Participant provide certain information in writing; (ii) conducting telephone and/or video conferences to request certain information orally or via demonstration; (iii) manually testing Participant's Monitored Products to duplicate the user experience; and/or (iv) utilizing automated tools. 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, which shall be no more than a one-year period, and twice during each one-year 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 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 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

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

i. **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.

ii. **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.

iii. **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.

iv. **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.

v. **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.

2. Participant may collect an audio file containing a Child's voice without obtaining parental consent, if (i) the audio file is used solely as a replacement for written words, such as to perform a search, to fulfill a verbal instruction or request, or to otherwise effectuate speech-to-text functionality in a Monitored Product; (ii) Participant only maintains the audio file for the brief time necessary for that purpose; and (iii) Participant provides clear notice of its collection and use of audio files and its deletion policy regarding the same. This exception, however, shall not apply if Participant requests information via voice that would otherwise be considered PID, such as a name.

3. Participant may collect a persistent identifier from a Child without providing direct notice to a parent or obtaining parental consent, if (i) Participant does not collect any other PID from the Child; and (ii) the persistent identifier is used for the sole purpose of providing support for the internal operations of the Monitored Product.

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 shall 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.