835 Market Street, Suite 800• San Francisco, CA 94103• Web: www.truste.com

March 22, 2017

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: Submission of TRUSTe's Proposed Post-Approval Modifications to its Children's Privacy Program under 16 CFR §312.11(e).

Dear Mr. Clark,

TRUSTe has operated a COPPA safe harbor program for over fifteen years, following its approval by the Federal Trade Commission (the "Commission") in May 2001 as the third approved COPPA safe harbor program. Since July 1, 2013, the date on which the amended COPPA Rule became effective, TRUSTe has certified over 60 unique companies as participants in its COPPA safe harbor program and more than one thousand companies across all of our certification and verification programs.

As a privacy solutions provider that combines expertise, methodology and technology to help organizations design, assess and demonstrate their privacy practices, TRUSTe appreciates the role that third party review and certification provides in enhancing transparency and trust in how privacy is protected online and around the globe. As one of the longest-serving certification providers in the global privacy ecosystem, TRUSTe has helped define the role of a privacy certification body not only in the U.S., where we are headquartered, but also across other regions of the world – from North America, to Asia Pacific, to Europe and Latin America – where our certification participants and/or their customers are based.

Privacy and data protection laws, technology and consumer expectations continue to change, and we recognize that certification and verification standards must evolve with them. We take our responsibilities as a leading provider of privacy certification solutions very seriously. Through time and the lessons of experience, we have learned how to operate and continually improve the privacy certification and verification programs we offer for a variety of purposes. Where we have made mistakes, we have addressed them promptly and implemented governance, process and technology-driven enhancements to detect and prevent future issues. While we learn from experience, we do not rely on the past to define our future. We believe that the next generation of standards for privacy accountability is still being defined, and we hope to continue as one of the

leading providers to help organizations demonstrate accountable privacy practices. Accordingly, we have been an active participant in the regulatory and policy dialogue related to organizational privacy accountability and compliance both within jurisdictions and across country borders. We have and will continue to work to build bridges for interoperable privacy and data protection standards across regions.

TRUSTe has provided and continually improved upon certification and verification programs for a range of privacy purposes, including but not limited to: certification and verification programs with a regulatory nexus, such as our COPPA safe harbor program, our APEC Cross-Border Privacy Rules ("CBPR") program, our former U.S.-EU and U.S.-Swiss Safe Harbor Privacy verification programs and our current Privacy Shield verification programs; certification programs addressing various technologies, such as our current certification programs for online advertising, downloadable software and the smart grid, and our former program for cloud service providers; and certification programs for enterprises generally seeking to demonstrate accountable privacy practices.[1] The rigor of our certification programs is based not only upon our certification standards, which we continue to improve upon, but also upon our commitment to continually learn from and enhance our program implementation based upon our practical experiences with program participants, new technologies affecting privacy expectations, changing organizational and supply chain practices, and evolving regulatory expectations.

Consistent with our commitment to continuous improvement, TRUSTe implemented operational enhancements to our certification-related business processes prior to entering into our Decision and Order with the Commission in March 2015 (the "Order").[2] Since that time, we have continued to enhance our overall certification and verification operations in a number of ways, such as migrating from interview-based reviews to technology-driven certification assessments completed by participants and enhancing the technology controls behind the privacy seals we award to our certification program participants and the associated certification validation pages for those participants. We also have improved our internal governance to ensure our integrity and the independence of our certification solutions, such as through the adoption and continuous improvements to our conflict of interest policies.

Following the changes to the COPPA Rule published in January 2013, TRUSTe updated its COPPA safe harbor program to conform to the amended Rule, and as an existing COPPA safe harbor provider, submitted its update to the Commission in June 2013.[3] Among other things, our amended program requirements included a revised definition of "Personal Information" that included persistent identifiers, such as cookies, where they can be used to recognize a user over time and across different websites or online services, not only where they were combined with individually identifiable information, as in the original COPPA Rule.

As required by the amended COPPA Rule, and as supplemented by our Order, TRUSTe has annually filed reports with the Commission pursuant to 16 CFR §312.11(d)(1). In our two most recent reports filed July 1, 2015 and July 1, 2016, respectively, TRUSTe described our COPPA assessment methodologies, including our proprietary scanning technology, originally released in 2012, which we use to identify tracking technologies,

[1] Details regarding TRUSTe's current certification programs are available at https://www.truste.com/privacy-certification-standards/.
[2] Docket C-4512
[3] Available at https://www.ftc.gov/system/files/attachments/press-releases/truste-earns-safe-harbor-status/130701tustecoppaapplication.pdf

such as cookies, flash cookies, web beacons and pixel tags. Our automated scanning technology functions by crawling web pages via a web browser and is used to identify the types of trackers found on a participant's websites, whether they are first or third party trackers and the categories of third party trackers, such as ad networks, analytics and service providers, data collectors and social media tools. TRUSTe monitors changes in web development as well as errors and malfunctions to continually update and enhance the automated scanner to address identified or potential limitations. Since the original release of our automated scanning technology in 2012 through the date of this submission, we have released 76 updates to this technology, including 35 updates since we entered into the Order. Since March 2015, based on our evaluation of ongoing changes in website development as well online technologies, we also have implemented supplemental manual scanning methods, where we have deemed them to be appropriate. In addition to our ongoing efforts to address the changing technical nature of online privacy risks, we continued to improve our COPPA safe harbor program processes in 2016 with the introduction of a dedicated technical analyst team for conducting the scans and by development of a technology-driven COPPA certification assessment completed by participants, which replaced the manual Children's Privacy Certification interview form previously used to gather information from program participants.

Pursuant to our current Children's Privacy Program Requirements, TRUSTe maintains the integrity of its COPPA safe harbor program through annual certification, by suspending participants for material violations of its Program Requirements, and by terminating participants for material breaches of the Program Requirements. Since July 1, 2013, TRUSTe has taken enforcement actions against 16 (or approximately one quarter) of the over 60 unique companies that have participated in our COPPA safe harbor program during that time.

In August 2015, the New York State Office of the Attorney General ("NYAG") commenced an inquiry related to two former participants in our COPPA safe harbor program and issues that predated the Order.[4] The NYAG expanded its investigation into our COPPA safe harbor program in December 2015. In order to minimize further disruption to our business and to our customers, we have agreed to resolve this matter by entering into a settlement, pursuant to which we have formally agreed to continue the operational and technical processes described above related to scanning for third party tracking technologies and to clarify certain of our policies and operating procedures related to third party tracking technologies in connection with our COPPA safe harbor program. As described below, the changes we have agreed to with the NYAG necessitate that we amend our current Children's Privacy Program Requirements to incorporate explicit requirements of the NYAG related to third party tracking and display of the TRUSTe Kids Privacy Seal.

Proposed Changes to TRUSTe Children's Privacy Certification Standards

While our COPPA safe harbor program is a small part of our certification business and a very small part of our overall privacy solutions business, because we believe in the value that third party review and certification provides in enhancing transparency and trust in how children's privacy is protected online and, further, because we believe the COPPA safe harbor program serves as an important accountability model for privacy

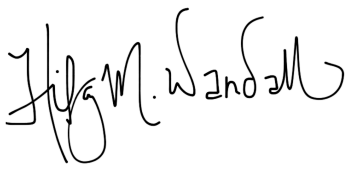
[4] In September 2016, the NYAG announced settlements with four companies in connection with its investigation into violations of COPPA. *See* https://ag.ny.gov/press-release/ag-schneiderman-announces-results-operation-child-tracker-ending-illegal-online.

certification of products and services, in particular those offered online, we are seeking the Commission's review and approval to amend our current Children's Privacy Program Requirements pursuant to 16 CFR §312.11(e) so that we can continue to offer the program to our current participants as well as to others who may seek to demonstrate their accountability in accordance with the regulatory enforcement expectations of the Commission.

For consistency with our other certification programs, we have renamed our program requirements as our "Children's Privacy Certification Standards." An annotated version of the proposed updated version of our Children's Privacy Certification Standards is set forth in Exhibit A. As described in detail in Exhibit A, TRUSTe is making substantive changes to our Children's Privacy Certification Standards to address regulatory expectations related to: (1) third party tracking technologies and (2) the timing for seal removal for participants who have not completed annual review and remediation by the anniversary of the prior year certification date. TRUSTe also is making structural changes to its Children's Privacy Certification Standards to align them with the TRUSTe Enterprise Privacy Certification Standards since many participants in our COPPA Safe Harbor program also participate in the TRUSTe Enterprise Privacy Program. Requirements of the Children's Privacy Certification Standards that are fundamental to COPPA are unchanged. The newly added or revised requirements meet or exceed COPPA requirements.

We look forward to the Commission's review and consideration of our proposed changes to our Children's Privacy Certification Standards and the opportunity to continue our service as a COPPA Safe Harbor program provider.

Sincerely,



Hilary M. Wandall, Esq.
General Counsel and Chief Data Governance Officer
TRUSTe

Exhibit A
Children's Privacy Certification Standards
With Annotations

TRUSTe is making substantive changes to its Children's Privacy Certification Standards (the "Standards") to address regulatory expectations related to: (1) third party tracking technologies and (2) the timing for seal removal for participants who have not completed an annual review and remediation by the anniversary of the prior year certification date. The substantive changes to the Standards are set forth in Section II, Minimum Program Requirements, under Data Governance and Participant Accountability.

TRUSTe is also making structural changes to the Standards to align them with the TRUSTe Enterprise Privacy Certification Standards since many TRUSTe Children's Privacy Program participants also participate in the TRUSTe Enterprise Privacy Program.

Requirements of the Standards that are fundamental to COPPA are unchanged. Newly added or revised requirements meet or exceed COPPA requirements.

The structural changes are summarized in the following table. Sections with substantive changes are noted with an (*)

.

Existing Standards	Revised Standards
I. Introduction	I. Program Description
II. Structure	
III. Definitions	II. Minimum Program Requirements • Privacy Notice • Privacy Practices ○ Online Behavioral Advertising • Data Governance* • Participant Accountability*
IV. Minimum Program Requirements • Participant Accountability • Privacy Practices • Privacy Statement • Data Governance • Online Behavioral Advertising	III. Definitions

A table of contents has been added to make it easier to reference the sections and sub-sections of these Standards. Sections containing changes have been noted for reference in this Annotated Version.

Table of Contents

Section I has been updated with a new header, Program Description, and now incorporates Section I, Introduction and Section II, Structure, from the previous version of the Standards.

I. Program Description

TRUSTe's Children's Privacy Program is designed for businesses that

a. Have actual knowledge they **collect personal information** ("PI") from **children** under the age of 13;

b. Offer websites or online services directed at or targeted towards **children** under age 13; or

c. Have actual knowledge they are **collecting** PI directly from the users of a website or online service directed at or targeted towards **children**.

The following criteria, in its totality, is used to determine whether an online service or a portion of an online service is targeted towards **children** under the age of 13:

a. Subject matter;

b. Visual content;

c. Use of animated characters or **child**-oriented activities and incentives;

d. Music or other audio content;

e. Age of models;

f. Presence of **child** celebrities or celebrities who appeal to **children**,

g. Language or other characteristics of the Web site or online service; and

h. Whether advertising promoting or appearing on the Web site or online service is directed to **children**.

TRUSTe will also consider information about audience composition and intended audience when determining whether an online service or a portion of an online service is directed towards **children** under age 13.

The following paragraph has been revised from language formerly set forth in Section II, Structure, of the prior version of the standards. The language has been updated to reflect modernization of certain practices, such as reference to a "seal" instead of a "trustmark" as well as TRUSTe's use of a certification validation page linked from the seal that describes the participant's certification scope. The intent of the language in this version remains the same as the intent of the language in the prior version. For reference, the prior language stated, "TRUSTe's programs certify how businesses collect and manage personally identifiable information. For a business to obtain a TRUSTe certification the business must provide proof of its privacy and data governance practices as those practices relate to the notice, choice, and accountability frameworks around the personally identifiable information it collects on behalf of its users, customers, and partners. These practices must reach a minimum standard as defined by TRUSTe's Program Requirements. Upon satisfactory evaluation, TRUSTe offers a certification trustmark for businesses that successfully achieve and maintain practices that are compliant with TRUSTe's standard."

In order for a business to successfully obtain a TRUSTe **Children**'s Privacy Certification, the business must provide to TRUSTe access to all relevant information and evidence demonstrating the existence and implementation of its privacy and data governance practices to be evaluated against these Certification Standards. Upon satisfactory evaluation, TRUSTe offers a **children**'s privacy certification seal and **validation page** that attests to the business's compliance with these Certification Standards.

Defined terms appearing in Section II of these Certification Standards are bolded when they appear in this document.

The prior version of the Standards included a Definitions section here. Definitions have now been moved to Section III at the end of these revised Standards.

II. Minimum Program Requirements

The following introductory paragraph has been modernized from its prior version to be consistent with these revised Standards and TRUSTe's overall practices. The intent of the language remains the same. For reference, the prior language stated, "All Participants wanting certification that their Online information collection and use practices comply with TRUSTe's Children's Privacy Program Requirements must comply with the following requirements:"

Any **Participant** seeking certification that their privacy polices and practices comply with TRUSTe's Children's Privacy Certification Standards shall demonstrate compliance with the following:

As set forth in the table above, this section has be reordered and now has only 4 sub-sections since the Online Behavioral Advertising content has been incorporated into the Privacy Practices sub-section.

The Privacy Notice section has been relabeled from the prior version in which the section was labeled Privacy Statement. As described in the Definitions section below, the definition has been updated as well. All references in the prior version to a Statement have been replaced in this version by the term Notice. The updated section no longer includes requirements for Short and Just-in-Time notices because these are optional types of privacy notices, the requirements were too prescriptive and these types of notices are not required under COPPA.

A. Privacy Notice

1. **Participant** shall maintain and abide by an accurate up-to-date **Privacy Notice** approved by TRUSTe, in its sole discretion, that states **Participant**'s information practices, and is in conformance with these Certification Standards including, but not limited to:

In this sub-section, the words "Personal Information" have been inserted in front of the acronym PI.

a. What information is **collected**, either through active or passive means, including whether the **Participant** enables the **Child** to make **Personal Information (PI)** publicly available; the types of entity(ies), including **Service Providers**, **collecting** PI on the **Participant**'s website or **online** service; and how **collected** PI is used;

b. What types of **Third Parties** and **Service Providers** PI is shared with and that those **Third Parties** and **Service Providers** have agreed to maintain the confidentiality, security, and integrity of the information;

c. The names of all **Operators**, who directly **collect** or maintain data from **Children** through the online property;

d. Whether PI is appended with information obtained from **Third Party** sources;

e. How and when the **Individual** can exercise choice as required in these Certification Standards;

f. How the **Individual** can request access to their information as required in these Certification Standards;

g. That **Parents** have the right to the following:

(1) Consent to the **Participant**'s **collection** and use of PI from a **Child** without also consenting to its **disclosure** to **Third Parties**, and a Notice of the procedure for exercising that right;

(2) Review PI **collected** from the **Child**, and a Notice of the procedure for exercising that right; and

(3) Have that PI **deleted** or to refuse further **collection** and use of the PI **collected** from the **Child**, and a Notice of the procedure for exercising that right;

The following sub-section has been expanded to include a requirement to describe information retention policies.

h. A general description of the **Participant**'s information retention policies, and the types of information security measures in place to protect **collected** PI or **Third-Party PI** as required in these Certification Standards;

The following sub-section has been expanded to provide examples of tracking technologies.

i. What tracking technologies (e.g., cookies, device-recognition technologies) are used by the **Participant** or other **Operators** on their website or online service and the purpose for using those technologies;

j. How the **Individual** can contact the **Participant** and any other **Operators collecting** PI from the **Child** on the **Participant**'s online property, including company name, phone number, email address or a link to an online form, and physical address. The **Participant** may list the name, address, phone number, and email address of one entity who will respond to all inquiries from **parents** concerning the privacy policies and use of **Children**'s information through the **Participant**'s website or online service;

k. How the **Individual** will be notified of any **material changes** in the **Participant**'s privacy practices and that the **Participant** will obtain new consent from the **Parent** prior to implementing a **material change** to information **collected** from a **Child**;

l That **collected** information is subject to disclosure pursuant to judicial or other government subpoenas, warrants, orders, or if the **Participant** merges with or is acquired by a **Third Party**, or goes bankrupt;

m. Effective date of **Privacy Notice**; and

The following sub-section combines two sub-sections previously labeled n) and o) in the prior version. The combined sub-section removes the TRUSTe participation scope disclosure requirement from the privacy notice and replaces it with a requirement to provide clear and conspicuous access to the TRUSTe Validation Page, now a defined term. The TRUSTe Validation Page will include information about the certification scope and participation in the TRUSTe program. This change reduces the risk to TRUSTe and the participant of misrepresentations regarding the status of participation in the TRUSTe program by enabling TRUSTe to control posting of the seal and content of the linked validation page as well as removal the seal from the online property of a non-compliant participating company or a terminated participant.

n. **Clear and conspicuous** access to the **Validation Page**, as outlined in TRUSTe's seal usage guidelines, and how to contact TRUSTe to express concerns regarding **Participant**'s **Privacy Notice** or privacy practices.

2 At a minimum, **Participant** shall link to a comprehensive **Privacy Notice** that **discloses** the **Participant**'s information practices.

3 Access to the **Privacy Notice** shall be clear and conspicuous and easily accessible.

4 **Privacy Notice** must be available when the **Individual** first engages with the **Participant**, such as through an application, website homepage or landing page.

5 **Privacy Notice** must be available at the point where the **Individual** provides PI, or through common footer accessible on every page.

6 **Participant** shall treat all **collected** information in accordance with the posted **Privacy Notice** in effect at the time of **collection** unless the **Parent** otherwise has given verifiable parental consent to the non-conforming treatment.

7 Foreign Language Privacy Notice

The following sub-section a. is new.

a. The **Privacy Notice** must be provided in the same language in which the **Participant**'s business operates.

The following sub-section consolidates sub-section a) and b) in the prior version and removes the association between the Foreign Language Privacy Notice and any English notice provided by the participant. The obligation for the Foreign Language Privacy Notice to accurately represent the participant's practices remains.

b. If **Participant** seeks TRUSTe certification of a **Privacy Notice** in a language other than English, TRUSTe will use reasonable efforts to verify that **Participant**'s **Foreign Language Privacy Notice** accurately describes the **Participant**'s privacy practices and meets the **Participant**'s obligations under these Certification Standards.

The following sub-section now includes a cross-reference to the sub-section on Material Changes under Privacy Practices below.

c. **Participant** must notify TRUSTe of any **Material Changes** to its **Foreign Language Privacy Notice** and submit changes to TRUSTe for review and approval as required in Section II.B.15.c) of these Certification Standards.

B. Privacy Practices

1. Collection Limitation

   a. **Participant** shall only **collect Personal Information** (PI) from a **Child** through its website or **Online** service if:

      (1) The **Participant** has provided notice to the **Parent** and has obtained verifiable parental consent as described in these Certification Standards prior to the **collection** of PI; or

      (2) The **collection** falls under an exception to verifiable parental consent as described in these Certification Standards.

   b. **Participant** must not require or entice a **Child**, by the prospect of a game, prize or other activity, to divulge more PI than is needed to participate in such activity.

2. Use of Information Collected from a Child

   a. **Participant** shall only use a **Child**'s PI in accordance with their posted **Privacy Notice** in effect at the time of **collection**.

   b. **Participant** shall only use a **Child**'s PI for:

      (1) The provision of those services described in the notice provided to the **Parent** and that the **Parent** has consented to; or

      (2) A use that falls under an exception to verifiable parental consent as described in these Certification Standards.

3 Verifiable Parental Consent

   a. **Participants** covered under this section must obtain verifiable parental consent prior to the **collection** of PI from a **Child**, unless an exception from Section II.B.4 below applies.

   b. **Participant** must give the **Parent** the option to consent to the **Participant**'s **collection** and use of the **Child**'s PI without consenting to the **disclosure** of the **Child**'s PI to **Third Parties**.

   c. **Participant** must use one of the following methods to obtain verifiable parental consent:

(1) A consent form signed by the **Parent** and returned to the **Participant** by postal mail, facsimile, or electronic scan (e.g., a .PDF file attached to an email);

(2) Require a **Parent**, in connection with a monetary transaction, to use a credit card, debit card, or other **online** payment system that requires username and password, or other authentication, that provides notification of each discrete transaction to the primary account holder;

(3) Have a **Parent** call a toll-free telephone number staffed by trained personnel;

(4) Have a **Parent** connect to trained personnel via video-conference;

(5) Verify a **Parent**'s identity by checking a form of government-issued identification such as driver's license number or last four digits of a social security number against databases of such information.

(a) The **Participant** must promptly **delete** the **Parent**'s identification from its records after such verification is complete.

(6) A verifiable parental consent mechanism that has been reviewed and approved by TRUSTe.

d. Verifiable **parent** consent can be obtained using email coupled with additional steps to provide assurances that the person providing the consent is the **Parent** if the **Participant** does not **disclose**, share, rent, or transfer a **child**'s PI to **Third Parties**.

(1) Such additional steps include one of the following:

(a) Sending a confirmatory email to the **Parent** following receipt of consent; or

(b) Obtaining a postal address or telephone number from the **Parent** and confirming the **Parent**'s consent by letter or telephone call.

(2) **Participant** that uses this method must provide notice to the **Parent** explaining that the **Parent** can revoke any consent given in response to the earlier email.

e. The notice provided to the **Parent** when **Participant** seeks verifiable parental consent must state the following:

(1) That the **Participant** has **collected** the **Parent**'s **Online Contact Information** from the **Child** in order to obtain the **Parent**'s consent;

(2) The purposes for which the **Participant** is seeking to **collect** PI from the **Child**;

(3) That the **Parent**'s consent is required for the **Child**'s participation in the **Participant**'s **online** property, and that the **Participant** will not **collect**, use, or **disclose** any PI from the **Child** if the **Parent** does not provide such consent;

(4) The additional items of PI the **Participant** intends to **collect** for the **Child**, or the potential opportunities for the disclosure of PI, if the **Parent** provides consent;

(5) A link to the **Participant**'s **Privacy Notice**;

(6) How the **Parent** can provide verifiable consent to the **collection**, use, and disclosure of the information; and

(7) That the **Participant** will **delete** the **Parent**'s **Online Contact Information** from its records if the **Parent** does not provide consent within a reasonable time from the date the direct notice was sent.

f. The **Participant** must make reasonable efforts, taking into consideration available technology, to ensure that the **Parent** receives notice.

g. The **Participant** who offers **online** services through schools and **collects** PI from a **Child** may rely on the school to act as an intermediary for obtaining verifiable **parent**al consent and provide that consent on behalf of the **Parent**.

(1) The **Participant** must take commercially reasonable measures to verify the school or the teacher providing consent is in fact a school or a teacher.

(2) **Participant** needs to ensure the school is providing the **parent** notice.

4 Exceptions to Verifiable Parental Consent

a. Verifiable parental consent to **collect** PI from the **Child** is not required to:

(1) Provide voluntary notice to the **Parent** about, and subsequently update the **Parent** about, the **Child**'s participation in the **Participant**'s **online** property which *does not* otherwise **collect**, use, or **disclose** the **Child**'s PI.

(a) The **Participant** may **collect** the **Parent**'s **Online Contact Information** from the **Child**, where;

(i) The **Parent**'s **Online Contact Information** may not be used or **disclosed** for any other purpose.

(ii) The **Participant** must make reasonable efforts, taking into consideration available technology, to ensure that the **Parent** receives the notice.

(b) Notice to the **parent** must state the following:

(i) That the **Participant** has **collected** the **Parent**'s **Online Contact Information** from the **Child** in order to:

(a) Provide notice to the **Parent**; and

(b) Subsequently update the **Parent** about the **Child**'s participation on the **Participant**'s **online** property;

(ii) The **Participant** does not otherwise **collect**, use, or **disclose** PI from the **Child**;

(iii) The **Parent**'s **Online Contact Information** will not be used or **disclosed** for any other purpose;

(iv) That the **Parent** may refuse to permit the **Child**'s participation on the **Participant**'s **online** property;

(v) That the **Parent** may require the deletion of the **Parent**'s **Online Contact Information**, and how the **Parent** can do this; and

(vi) Have a link to the **Participant**'s **Privacy Notice**.

(2) Provide notice and obtain parental consent about, and subsequently update the **Parent** about, the **Child**'s participation in the **Participant**'s **online** property which *does* **collect**, use, or **disclose** the **Child**'s PI.

(a) The **participant** may **collect** the **Parent** or **Child**'s **Online Contact Information**, where;

(i) **Online Contact Information** is not used for any other purpose.

(ii) The **Participant** must **delete** the **collected** information from its records if the **Participant** has not received parental consent after a reasonable time from the date the information was **collected**.

(b) Notice to the **Parent** must state the following:

(i) That the **Participant** has **collected** the **Parent**'s **Online Contact Information** and, if such is the case, the name of the **Child** or **Parent** from the **Child** in order to obtain the **Parent**'s consent;

(ii) That the **Parent**'s consent is required for the **Participant** to **collect**, use, or **disclose** information from the **Child**, and that the **Participant** will not **collect**, use, or **disclose** any PI from the **Child** if the **Parent** does not provide such consent;

(iii) The additional items of PI the **Participant** intends to **collect** from the **Child**, or the potential opportunities for the disclosure of PI, if the **Parent** provides consent.

(iv) Have a link to the **Participant**'s **Privacy Notice**;

(v) How the **Parent** can provide verifiable consent to the **collection**, use, and disclosure of the information; and

(vi) The **Participant** will **delete** the **Parent**'s **Online Contact Information** from its records if the **Parent** does not provide consent within a reasonable time from the date the direct notice was sent.

(3) Respond directly on a one-time basis to a specific request from the **Child**.

(a) The **Participant** may **collect** the **Child**'s **Online Contact Information**, without notice, where the **Child**'s **Online Contact Information** is (i) not used to re-contact the **Child** or for any other purpose; (ii) not **disclosed** to **Third Parties**; and (iii) **Deleted** by the **Participant** from its records promptly after responding to the **Child**'s request.

(4) Respond directly more than once to the **Child**'s specific request.

(a) With notice, the **Participant** may **collect** the **Child**'s and **Parent**'s **Online Contact Information** for the purpose of facilitating multiple direct **online** communications at the request of the **Child** (e.g. a monthly newsletter), where the **Online Contact Information collected** under this exception is not to be used for any other purpose, **disclosed**, or combined with any other information **collected** from the **Child**.

(b) Notice to the **Parent** must state the following:

(i) The **Participant** has **collected** the **Child**'s **Online Contact Information** from the **Child** in order to provide multiple **online** communications (e.g. email) to the **Child**;

(ii) The **Participant** has **collected** the **Parent**'s **Online Contact Information** from the **Child** in order to notify the **Parent** that the **Child** has registered to receive multiple **online** communications (e.g. email) from the **Participant**;

(iii) The **Child**'s **Online Contact Information** will not be used for any other purpose, **disclosed**, or combined with any other information **collected** from the **Child**;

(iv) The **Parent** may refuse to permit further contact with the **Child** and require the deletion of the **Parent**'s and **Child**'s **Online Contact Information**, and how the **Parent** can do so;

(v) If the **Parent** fails to respond to this direct notice, the **Participant** may use the **Child**'s **Online Contact Information** for the purpose stated in the notice; and

(vi) Have a link to the **Participant**'s **Privacy Notice**.

(c) The **Participant** must make reasonable efforts, taking into consideration available technology, to ensure that the **Parent** receives the notice.

(i) If the **Parent** fails to respond to this direct notice, the **Participant** may use the **Child**'s **Online Contact Information** for the purpose stated in the notice.

(ii) The **Participant** will not be deemed to have made reasonable efforts to ensure that a **Parent** receives notice where the notice to the **Parent** was unable to be delivered.

(5) Protect the safety of the **Child**.

(a) With notice, the **Participant** may **collect** a **Child**'s name and the **Child** and **Parent**'s **Online Contact Information**, where the **Online Contact Information** is not used or **disclosed** for any purpose unrelated to the **Child**'s safety.

(b) Notice to the **Parent** must state the following:

(i) The **Participant** has **collected** the **Child**'s name and the **Online Contact Information** of the **Child** and the **Parent** in order to protect the safety of a **Child**;

(ii) The information will not be used or **disclosed** for any purpose unrelated to the **Child**'s safety;

(iii) The **Parent** may refuse to permit the use, and require the deletion of, the information **collected**, and how the **Parent** can do this;

(iv) The **Participant** may use the information for the purpose stated in the notice if the **Parent** fails to respond to the notice; and

(v) Have a link to the **Participant**'s **Privacy Notice**.

(c) The **Participant** must make reasonable efforts, taking into consideration available technology, to provide a **Parent** with notice.

(6) **Collect** only the **Child**'s name and **Online Contact Information**, to be used only for the following purposes and no other purposes:

(a) Protect the security or integrity of its **online** property;

(b) Take precautions against liability;

(c) Respond to judicial process; or

(d) To the extent permitted under other provisions of law, to provide information to law enforcement agencies, or for an investigation on a matter related to public safety.

(7) **Collect** and use of a persistent identifier for providing **Support for the Internal Operations** of the **online** property, as long as:

(a) No other PI is **collected**; and.

(b) The persistent identifier is not used for any other purpose.

(8) If the **Participant** has actual knowledge it is **collecting** PI from users of another website or **online** service **directed to children**, the **Participant** may **collect** a persistent identifier and no other **Personal Information** from a user who affirmatively interacts with the **Participant** and whose previous registration with that **Participant** indicates that such user is not a **Child**.

5 Collection and Use of Third Party PI

a. **Participant** shall use **Third Party** PI **collected** solely to facilitate the one-time completion of the transaction for which the PI was **collected**.

b. **Participant** must obtain verifiable parental consent from the **Parent** of the **Child** to whom such **Third Party** PI pertains before such **Third Party** PI may be used, **disclosed**, or distributed by the **Participant** for any other purpose.

c. Regarding **Third Party** PI the **Privacy Notice** shall state:

(1) The types of entities **collecting Third Party** PI;

(2) What kind of **Third Party** PI is **collected**, either through active or passive means;

(3) How **collected Third Party** PI is used and/or **disclosed**; and

(4) What types of additional **Third Parties** if any, including **Service Providers**, **collected Third Party** PI is shared with.

6 Access

a. **Parents** have the right to request access to the information the **Participant** has **collected** from the **Child**. The **Participant** must implement a reasonable and appropriate mechanism that allows the **Parent** to do the following:

(1) Review a description of the specific types or categories of PI **collected** from **Children** by the **Participant**.

(2) Review what information has been **collected** from the **Child**.

(3) Correct and update inaccurate information **collected** from the **Child**.

(4) Request that the information **collected** from the **Child** be **deleted**.

(5) Refuse the further use or future **online collection** of **personal information** from that **Child**.

b. Such mechanism or process should be consistent with how the **Individual** normally interacts or communicates with the **Participant**.

c. Such mechanism or process shall be clear, conspicuous, and easy to use.

d. Such mechanism or process shall confirm to the **Individual** inaccuracies have been corrected.

e. **Participant**'s **Privacy Notice** shall state how access is provided.

f. Any means employed by the **Participant** to permit the review by a **Parent** of the PI **collected** from the **Child** must:

(1) Ensure that the requestor is a **Parent** of that **Child**, taking into account available technology; and

(2) Not be unduly burdensome to the **Parent**.

g. If **Participant** denies access to PI, **Participant** must provide the **Individual** with an explanation of why access was denied and contact information for further inquiries regarding the denial of access

(1) In the case of information **collected** from a **Child**, the **Participant** must provide the **Parent** an explanation of why access was denied and contact information for further inquiries.

7 Mixed Audience Websites and Online Services

a. **Participants** offering a **Mixed Audience Website and Online Service** may employ an age screen.

(1) The **Participant** must not **collect** PI from any **Individual** prior to the age screen.

(2) The age screen mechanism must allow **Individuals** to accurately enter their age information.

(3) **Participant** must not encourage an **Individual** to falsify their age information.

(4) The **Participant** cannot use the age screen to block **Children**.

b. Upon identifying an **Individual** as a **Child**, the **Participant** may:

(1) **Collect Parents**' **Online Contact Information** to provide direct notice of **Participant**'s information practices and obtain **Parents**' consent, as described in Sections II.B.3 and II.B.4; or

(2) Direct the **Child** to content that does not involve the **collection**, use, or disclosure of PI.

8 Promotional and Newsletter Email Communications

a. All newsletters and promotional email messages that **Participant** sends to the **Individual** must include **Participant**'s postal address and a functional unsubscribe mechanism.

b. The location and instructions concerning the unsubscribe mechanism must be Clear and Conspicuous, and the mechanism itself must be functional for no fewer than thirty (30) days following the sending of the newsletter or promotional email message.

c. **Participant** must honor the **Individual**'s request to unsubscribe from a newsletter or promotional email message beginning on the tenth (10) business day after the **Participant** receives the unsubscribe request, unless the **Individual** subsequently requests to receive newsletters or promotional email messages from **Participant**.

(1) If a **Child** subsequently requests to receive newsletters or promotional email messages from the **Participant**, the **Participant** must send the **Parent** notice and obtain consent as required in these Certification Standards.

d. An unsubscribe mechanism is not required for administrative or customer service-related email messages (e.g. account management or provisioning of requested services, warranty or recall information, safety or security announcements).

9 Geo-location Information

a. **Participant** must obtain verifiable parental consent prior to the **collection** of geo-location information from a **Child**.

b. **Participant** shall use reasonable encryption methods for the transmission of geo-location information that is used to identify or describe the **Child**'s actual physical location at a given point in time.

10 Public Disclosure of PI

a. A **Participant** may allow a **Child** to post PI in an **online** forum, chat room, blog or other public forum, where the PI is displayed if the **Participant** has provided notice to the **Parent** and obtained verifiable parental consent.

(1) If appropriate and commercially reasonable, provide a process or mechanism to allow the **Individual** to

request timely removal of any publicly displayed PI where it has been legally and rightfully shared; and

(2) State in the **Privacy Notice** how the **Individual** can request removal of publicly displayed PI.

b. The **Privacy Notice** shall state information posted by **Children** in **online** forums, chat rooms, blogs, or other public forum may be displayed publicly.

c. The **Privacy Notice** shall accurately describe the extent to which a **Child**'s displayed PI is publicly available.

d. The **Participant** is not required to obtain verifiable parental consent if the **Participant** takes commercially reasonable measures to monitor and remove PI from the **Child**'s messages and postings prior to those messages and postings being made public or sent and also **Deletes** such information from its records.

11 Photos, Video, and Audio

a. **Participant** must obtain verifiable parental consent prior to allowing the **Child** to upload photos, videos, or audio files containing a **Child**'s image or voice.

b. A photo may be posted without verifiable parental consent if the **Participant** takes commercially reasonable measures to blur or remove images of any **Child** appearing in the photo, and remove and **Delete** from its records any metadata from the photo, prior to making the photo publicly available.

12 Screen Names

a. **Participant** must obtain verifiable consent if a **Child**'s screen name can be used as **Online Contact Information**.

b. Verifiable parental consent is not required if screen names that cannot be used as **Online Contact Information** are **collected** and used for:

(1) Content and service personalization;

(2) Filtered chat;

(3) Public display on an **online** service; or

(4) For use as a single login identifier to allow the **Child** to transition between devices or allow access to the **Participant**'s related **online** properties across multiple platforms.

c. Screen names may not contain a **Child**'s first name and last name or function as **Online Contact Information** without first obtaining verifiable parental consent.

13 Persistent Identifiers

a. **Participant** must obtain verifiable parental consent prior to the **collection** of persistent identifiers unless the persistent identifier has been **collected** under one of the exceptions as described in Section III.B.4.a)(7) and Section III.B.4.a)(8) of these Certification Standards.

b. **Participant** may use a persistent identifier, without verifiable parental consent, to **collect** information from a **Child** for the **Support of the Internal Operations** on **Participant**'s **online** service, including for personalization.

c. If the **Participant** has actual knowledge it is **collecting** PI from users of another website or **online** service **directed to children**, the **Participant** may **collect** a persistent identifier and no other **Personal Information** from a user who affirmatively interacts with the **Participant** and whose previous registration with that **Participant** indicates that such user is not a **Child**.

d. Persistent identifiers cannot be used to build a profile about the **Child** or for **Online Behavioral Advertising (OBA)** unless the **Participant** has first received verifiable parental consent.

As described above, this Online Behavioral Advertising content has been consolidated under this Privacy Practices sub-section. In the prior version, this content was a stand-alone sub-section under Minimum Program Requirements.

14 Online Behavioral Advertising (OBA)

a. **Participants** engaging in **OBA** shall **disclose** the following regarding **Participant**'s **OBA** Practices in its **Privacy Notice**:

(1) If information, **collected** either through active or passive means, is used by either the **Participant**, **Service Provider**, or **Third Party**(ies) for the purpose of **OBA**;

(2) If PI **collected** by the **Participant** is linked to information **collected** through web usage activity from other sources, e.g. websites other than **Participant**'s, for the purpose of **OBA**;

(3) Whether PI or **Third Party** PI is **collected** by, or shared with, additional **Third Parties** or **Service Provider**s for the purposes of **OBA**; and

(4) How and when the **Individual** can exercise choice as required in this Section II.B.14.

b. **Participant** shall provide instructions or link to a mechanism that enables the **Individual** or **Parent** to withdraw consent for the use of PI for **OBA**.

(1) At a minimum, such instructions or link shall be made available in the **Participant**'s **Privacy Notice**.

c. **Participant** must obtain verifiable parental consent prior to **collecting** PI from a **Child**, linking **collected** PI to **online** usage information, or disclosing PI to **Third Parties** or **Service Providers** for the purpose of **OBA**.

d. **Participant** must provide a mechanism for the **Parent** to review what PI the **Participant** has **collected** from the **Child**.

e. **Participant** must provide a mechanism for the **Parent** to withdraw consent, and to request deletion or no longer use PI **collected** from the **Child**.

f. The **Parent** must be provided an opportunity to withdraw consent to having the **Child**'s PI linked to information **collected** through **online** usage activity for the purpose of **OBA**;

g. The **Parent** must be provided an opportunity to withdraw consent to having the **Child**'s PI shared with **Third Parties** for the purpose of **OBA** at the time such PI is **collected**.

15 Material Changes

a. **Participant** must notify the **Individual** of any **Material Changes** to its PI **collection**, use, or disclosure practices prior to making the change.

b. If the **Individual** is a **Child**, **Participant** must notify the **Parent** and obtain verifiable parental consent prior to implementing any **Material Change** in the **collection**, use, or disclosure practices of PI **collected** from a **Child**.

c. **Participant** must obtain prior approval from TRUSTe:

(1) For any **Material Change** in its PI **collection**, use, or disclosure practices; and

(2) For notice method and content to the **Individual**, including the **Parent**, such as email, "in product" messaging, etc.

C. Data Governance

1 General Requirements

The language in the following sub-section was moved from the Participant Accountability section in the prior version and consolidated here. A requirement for "policies" was added to the existing requirement for "processes."

a. **Participant** shall have policies and processes in place to comply with these Certification Standards

b. **Participant** shall implement controls and processes to manage and protect PI within its control including the ones listed in this Section II.C

c. Such controls and processes shall be appropriate to the size of the **Participant**'s business; and appropriate to the level of sensitivity of the data **collected** and stored.

This sub-section was revised from the prior version to include additional requirements consistent with the TRUSTe Enterprise Certification Standards.

2 Data Security

a. **Participant** must implement commercially reasonable procedures to protect PI within its control from unauthorized access, use, alteration, disclosure, or distribution.

b. **Participant** must maintain and audit the internal information technology systems within its control such as:

This following sub-sections are new requirements: (1), (2) and (6)

(1) Authentication and access controls;

(2) Boundary protections measures (e.g., firewalls, intrusion detection);

(3) Regularly monitor and repair systems including servers and desktops for known vulnerabilities;

(4) Limit access and use of PI and Third-Party PI to Personnel with a legitimate business need where inappropriate access, use, or disclosure of such PI or Third-Party PI could cause financial, physical, or reputational harm to the **Individual**;

(5) Implement protection against phishing, spam, viruses, data loss, and malware;

(6) Implement processes for the deletion, return, or secure disposal of PI or Third-Party PI; and

(7) Use reasonable encryption methods for transmission of information across wireless networks, and storage of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an **individual**.

c. Access to PI or **Third Party** PI retained by **Participant** must be at least restricted by username and password if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an **Individual**.

d. **Privacy Notice** shall state that security measures are in place to protect **collected** PI and/or **Third Party** PI.

3 Data Quality

a. **Participant** shall take commercially reasonable steps when **collecting**, creating, maintaining, using, disclosing or distributing PI to assure that the information is sufficiently accurate, complete, relevant, and timely for the purposes for which such information is to be used.

b. If any information **collected** by the **Participant** about an **Individual** is disputed by that **Individual** (or their **Parent** where the **Individual** is a **Child**) and is found to be inaccurate, incomplete, or cannot be verified, **Participant** shall promptly **Delete** or modify that item of information, as appropriate, based on the results of the investigation.

4 Data Retention

This sub-section was revised from the prior version to include additional requirements consistent with the TRUSTe Enterprise Certification Standards. Specifically, the new language in a., which states"…necessary for uses not incompatible with the purposes of collection" replaces the language in the prior version which stated, "…commercially useful to carry out its business purpose, or legally required; and must disclose in their Privacy Statement its policies regarding information retention." The disclosure requirement has been moved to Section II.A.1.h. above.

a. If a **Participant** receives and retains PI or **Third Party** PI, the **Participant** must limit its retention to no longer than necessary for uses not incompatible with the purposes of **collection**. The **Participant** must **delete** such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

b. Regardless of the time period of retention, so long as a **Participant** has PI or **Third Party** PI in its possession or control, the requirements included herein shall apply to such information.

The following sub-section has been modified to incorporate the new substantive requirement for participants to conduct, at least annually, a comprehensive internal assessment to identify all third parties and service providers involved in collecting PI from children or receiving PI about children in order to address regulatory expectations regarding third party tracking technologies.

5 Third Parties and Service Providers

a. **Participant** shall, at least annually, conduct a comprehensive internal assessment to identify and evaluate all **Third Parties** and **Service Providers**, actively or passively **collecting** PI from **Children** through the **Participant**'s **online** property or with whom it shares PI in order to:

(1) Determine what information the **Third Party** or **Service Provider** will be **collecting** or maintaining from the **Child** or the **Participant**, and how that information will be used;

(2) Determine the types of PI the **Third Party** or **Service Provider** allows other **Third Parties** or **Service Providers** to **collect** and maintain; and

(3) Determine what measures the **Third Party** or **Service Provider** takes to protect and maintain the security and integrity of the information it **collects**.

b. **Participant** must take commercially reasonable steps to ensure that **Third Parties** and **Service Providers**, actively or passively **collecting** PI from the **Child** through the **Participant**'s **online** property, or with whom it shares PI:

(1) Abide by the rights and obligations attached to the PI by the **Participant** regarding the security, confidentiality, integrity, use, and disclosure of the PI; and

(2) If the **Parent** has requested the **Participant** to **Delete**

(3) PI **collected** from the **Child**, the **Participant** to the extent possible should take commercially reasonable measures to notify **Third Parties** and **Service Providers** with whom it may have **disclosed**, or otherwise shared the **Child**'s PI with, of the **Parent**'s request.

c. **Participant** must take reasonably commercial measures to require that **Service Providers** abide by privacy policies that are substantially equivalent to **Participant**'s privacy policies as reflected in **Participant**'s **Privacy Notice**.

This sub-section was newly added to include additional requirements consistent with the TRUSTe Enterprise Certification Standards.

6. Training

a. The **Participant** must conduct regular training of Personnel regarding:

(1) Maintaining the security, confidentiality, and integrity of PI and Third-Party PI it receives from an **Individual**;

(2) The **Participant**'s privacy policies and information **collection**, destruction, and use practices; and

(3) The **Participant**'s Business Continuity Plan and Disaster Recovery Program.

7. User Complaints and Feedback

a. **Participant** shall provide users with reasonable, appropriate, simple and effective means to submit complaints, express concerns, or provide feedback regarding **Participant**'s privacy practices.

b. **Participant** shall also cooperate with TRUSTe's efforts to investigate and resolve non-frivolous privacy complaints, questions and concerns raised either by:

(1) Users through TRUSTe's dispute resolution process; or

(2) TRUSTe.

8. Data Breach

a. Unless otherwise required or restricted by law; **Participant** must notify an **Individual** of a data breach concerning their PI or the PI of their **Child** within 45-days of a known breach.

b. Unless otherwise required by law, notice to the **Individual** must **disclose** the following:

(1) That a breach occurred;

(2) What type of information was breached;

(3) When the breach happened;

(4) What steps **Individuals** can take to protect themselves or their **children**;

(5) What actions the **Participant** is taking regarding the breach (e.g. investigation); and

(6) What steps the **Participant** is taking to ensure the event does not happen again.

c. **Participant** must notify TRUSTe when it believes a data breach occurred. **Participant** must provide TRUSTe a copy of the notice to be sent or sent to affected **Individual**(s)

As described above, this sub-section has been moved from the beginning of the Program Requirements section to its new placement here at the end.

D. **Participant** Accountability

This sub-section has been modified to further address implementation expectations supporting the new substantive requirement for participants to conduct, at least annually, a comprehensive internal assessment to identify all third parties and service providers involved in collecting PI from children or receiving PI about children in order to address regulatory expectations regarding third party tracking technologies.

1. Cooperation with TRUSTe

a. **Participant** shall provide, at no charge to TRUSTe or its representatives, full access to the **online** properties (e.g., including password access to premium or members-only areas) for the purpose of conducting reviews to ensure that **Participant**'s **Privacy Notice**(s) is consistent with actual practices.

This sub-section is new and supports TRUSTe's ability to conduct an accurate review of participant's practices.

b. The **Participant** shall provide, upon TRUSTe's reasonable request, information including copies of all relevant policies regarding how PI is gathered and used.

This sub-section has been enhanced to strengthen requirements for participant accountability for conducting due diligence on their own practices, documenting and providing accurate information about those practices to TRUSTe and attesting as to the same. It further supports TRUSTe's ability to address regulatory expectations regarding third party tracking technologies. The prior version only required that the participant "[p]rovide, upon TRUSTe's request, information regarding how PI gathered from and/or tracked through Participant's Online properties is used.

c. **Participant** shall conduct, at least annually, a comprehensive internal assessment of its practices related to **Third Parties** and **Service Providers** as described in Section II.C.5., and shall provide to TRUSTe in writing a description of how the assessment was conducted, the results of that assessment and an attestation that the assessment was conducted as described.

This sub-section was added to require participant to cooperate with TRUSTe's verification activities to ensure that participant's practices comply with TRUSTe's Certification Standards.

d. **Participant** shall cooperate with additional verification activities required by TRUSTe, as warranted based on the risk of **Participant**'s practices, to determine compliance with these Certification Standards, including periodic compliance monitoring, or third-party onsite audits, the costs for which shall be borne by the **Participant**.

This sub-section has been relabeled "Annual Review." In the prior version, it was called "Annual Certification." The revised sub-section introduces newly added requirements including a defined term for "Annual Review" as set forth in the Definitions section below, specifies the requirements for an Annual Review and identifies the consequences of not

completing the Annual Review and any required remediation by the prior year certification date.

2. Annual Review

a. The **Participant** shall undergo an **Annual Review** to verify ongoing compliance with these Certification Standards.

b. If issues of non-compliance with any of these Certification Standards are found as a result of such **Annual Review**, TRUSTe will Investigate the compliance issue, notify the **Participant**, outline the corrections necessary and provide a reasonable timeframe, not to exceed the **Participant**'s anniversary of the prior re-certification date, for the **Participant** to make such changes, during which time, TRUSTe will work with the **Participant** to ensure the necessary changes are made.

c. TRUSTe will discontinue the **Participant**'s certification, including removal of the TRUSTe Children's Privacy seal, if the **Participant** fails to provide the necessary information to enable TRUSTe to complete the Annual Review, to enable timely completion of the Annual Review, or to correct required changes by the anniversary of the prior year certification date.

This sub-section combines two separate sub-sections in the prior version labeled "Termination for Material Breach" and "Suspension Status." The new sub-section has been relabeled "Certification Status." A requirement has been added for TRUSTe to provide notice and immediately remove the seal if TRUSTe determines that the participant's certification has lapsed or that the participant has materially breached the Certification Standards.

3. Certification Status

a. In the event TRUSTe determines that **Participant**'s compliance with these Certification Standards has lapsed, TRUSTe will provide notice and immediately remove the TRUSTe Children's Privacy seal.

(1) TRUSTe may reinstate the **Participant**'s certification if the **Participant** makes all the required changes and demonstrates to TRUSTe's satisfaction that such changes have been implemented.

b. Upon notice to the **Participant**, TRUSTe may discontinue immediately the **Participant**'s certification, including removal of the TRUSTe Children's Privacy seal, if **Participant** is found in material breach of these Certification Standards. Material

breaches of these Certification Standards include but are not limited to:

(1) **Participant**'s continual, intentional, and material failure to adhere to these Certification Standards;

(2) **Participant**'s material failure to permit or cooperate with a TRUSTe investigation or review of **Participant**'s policies or practices pursuant to the Certification Standards;

(3) **Participant**'s material failure to cooperate with TRUSTe regarding an audit, privacy-related complaint, or the compliance monitoring activities of TRUSTe; or

(4) Any deceptive trade practices by the **Participant**.

As noted above, the following section has been moved from its earlier placement in the prior version.

III. Definitions

The following definitions shall apply herein (defined terms are noted in **bold** throughout these Standards):

The following definition is new. The precise term for annually re-certifying a participant was not defined in the prior version. Under our prior version of these Standards, our annual certification / re-certification lifecycle for COPPA commenced with the prior year's certification. Preparation for re-certification typically began approximately 9 months after the prior year's certification, however, the timing can be affected by other concurrent activities with the participant. For example, a new license for another certification product affecting the participant's website, modified scope of the existing license (such as expansion to mobile properties), and changes in the participant's or TRUSTe's personnel responsible for working on the certification, all of which can cause unexpected delays in the process. Historically, factors like the foregoing would not result in suspension of the seal unless TRUSTe had received and substantiated a consumer complaint that indicated participant's material non-compliance with the requirements, or TRUSTe had discovered a material compliance violation through our annual re-certification process that had not been remediated. In some cases, the re-certification lifecycle has been modified due to our suspension of a participant from our COPPA program until remediation of the issue resulting in the suspension has been completed. In these cases, the re-certification timeframe was based upon the date of the participant's re-entry into the program.

A. "Annual Review" is a process to check the **Participant**'s compliance with these Certification Standards. This process and re-certification of the

Participant must be completed by the anniversary of the prior year certification date.

B. "Clear and Conspicuous" means a notice that is reasonably easy to find, and easily understandable in terms of content and style to the average reader.

C. "Child(ren)" is an (are) **Individual**(s) under the age of 13.

D. "Collects" or "Collection" means the gathering of any PI from a **Child** by any means, including but not limited to:

1 Requesting, prompting, or encouraging a **Child** to submit **Personal Information** (PI) **online**;

2 Enabling a **Child** to make PI publicly available in identifiable form. An **Operator** shall not be considered to have **collected** PI if the **Operator** takes reasonable measures to **delete** all or virtually all PI from a **Child**'s postings before they are made public and also to **delete** such information from its records; or

3 Passive tracking of a **Child online**.

E. "**Delete**" means to remove PI such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

F. "**Disclose**" or "Disclosure" means, with respect to PI:

1. The release of PI **collected** by an **Operator** from a **Child** in identifiable form for any purpose, except where an **Operator** provides such information to a person who provides **Support for the Internal Operations** of the website or **online** service; and

2. Making PI **collected** by an **Operator** from a **Child** publicly available in identifiable form by any means, including but not limited to a public posting through the Internet, or through a personal home page or screen posted on a website or **online** service; a pen pal service; an electronic mail service; a message board; or a chat room.

G. "Directed to **Children**" means an **online** property (e.g. a website or **online** service) or a portion of an **online** property that is targeted towards **Children** as determined using the criteria listed in Section I of these Certification Standards

H. "Foreign Language **Privacy Notice**" is the **Participant**'s **Privacy Notice** translated into a language other than English.

I. "Individual" means the discrete person to whom the **collected** information pertains.

J. "Material Change" means change in the rights or obligations regarding the **collection**, use, or disclosure of PI for an **Individual** or that the **Parent** consented to. This usually includes changes to **Participant**'s:

1 Practices regarding notice, **collection**, use, and disclosure of PI and/or **Third Party** PI;

2 Practices regarding user choice and consent to how PI and/or **Third Party** PI is used and shared; or

3 Measures for information security, integrity, access, or **individual** redress.

K. "Mixed Audience Website or **Online** Service" is an **online** property that is Directed to **Children** but **Children** under 13 are not the primary audience.

L. "**Online**" is the state where an **Individual** is connected by computer or Mobile Device to one or more other computers, Mobile Devices, or networks, as through a commercial electronic information service or the Internet.

M. "Online Behavioral Advertising (**OBA**)" means the **collection** of data from a particular computer or device regarding an **Individual**'s **Online** viewing behaviors over time - including searches the **Individual** has conducted, web pages visited, and content viewed - for the purpose of using such data to predict **Individual** preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such **Online** viewing behaviors. **OBA** does not include contextual advertising where an ad is based upon a single web page visit or single search query.

N. "**Online Contact Information**" means an e-mail address or any other substantially similar identifier that permits direct contact with a person **online**, including but not limited to, an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.

O. "Operator" means any entity that operates a website or **online** service and who **Collects** or maintains PI from or about **Individuals**, or visitors to such website or **online** service, or on whose behalf such information is **collected** or maintained, or offers products or services for sale through that website or **online** service, where such website or **online** service is operated for commercial purposes. **Personal information** is **collected** or maintained on behalf of an **Operator** when:

1 It is **collected** or maintained by a **Service Provider** of the **Operator**; or

2 The **Operator** benefits by allowing another entity to **Collect** PI directly from a **Child** or other **Individuals** of such website or **online** service.

P. "Parent" is a legal guardian of a **Child**.

Q. "Participant" means any entity that entered into an agreement with TRUSTe to participate in the TRUSTe program(s) and agreed to comply with the Certification Standards included therein and 1) has been determined to be an **Operator** as defined in these Certification Standards of a website or online service Directed to **Children**; 2) has actual knowledge that it is **collecting** PI directly from users of another website or online service Directed to **Children**; or 3) has actual knowledge it is **collecting Personal Information** from a **Child**.

R. "Personal Information (PI)" means individually identifiable information about an **individual collected** online, including:

1 A first and last name;

2 A home or other physical address including street name and name of a city or town;

3 **Online Contact Information** as defined herein;

4 A screen or user name where it functions in the same manner as **Online Contact Information**, as defined herein;

5 A telephone number;

6 A Social Security number;

7 A persistent identifier that can be used to recognize a user over time and across different websites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier;

8 A photograph, video, or audio file where such file contains a **child**'s image or voice;

9 Geo-location information sufficient to identify street name and name of a city or town; or,

10 Information concerning the **child** or the **parents** of that **child** that the **Operator collects** online from the **child** and combines with an identifier described in this definition

The following definition was changed from "Privacy Statement" in the Prior Version to "Privacy Notice". Specific references to Short and Just in Time notices have been removed. These changes align this definition with TRUSTe's Enterprise Certification Standards.

S. "Privacy Notice" shall mean the notices, including a single, comprehensive notice, of the **Participant**'s information **collection** and usage practices; as such practices are updated from time to time.

T. "Service Provider" is anyone other than the **Participant** or the **Individual** who provides **Support for the Internal Operations** of the website or online service and who does not use or **disclose** the PI **collected** for any other purpose.

U. "Support for the Internal Operations" means those activities necessary to:

1. Maintain or analyze the functioning of the website or online service;

2. Perform network communications;

3. Authenticate users of, or personalize the content on, the website or online service;

4. Serve contextual advertising on the website or online service or cap the frequency of advertising;

5. Protect the security or integrity of the user, website, or online service;

6. Ensure legal or regulatory compliance;

7. Fulfill a one-time request of a **child** or for multiple contacts with a **child** as allowed in Section II.B.4; or

8. It is a use that has been reviewed and approved in advance by the FTC.

Information **collected** for the activities listed above may not be used or **disclosed** to contact a specific **individual**, including through Online Behavioral Advertising, to amass a profile on a specific **individual**, or for any other purpose.

V. "Third Party(ies)" is/are an entity(ies) other than the **Participant** or **Participant**'s **Service Providers**.

W. "Third Party Personal Information (Third Party PI)" means PI that is **collected** by **Participant** from a **Child** about another **Individual**.

X. "Validation Page" is a web page controlled and hosted by TRUSTe that verifies the **Participant**'s certification status, and the TRUSTe certification scope.