# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Program Description</td>
<td>2</td>
</tr>
<tr>
<td>II. Minimum Program Requirements</td>
<td>3</td>
</tr>
<tr>
<td>A. Privacy Notice</td>
<td>3</td>
</tr>
<tr>
<td>B. Privacy Practices</td>
<td>5</td>
</tr>
<tr>
<td>1. Collection Limitation</td>
<td>5</td>
</tr>
<tr>
<td>2. Use of Information Collected from a Child</td>
<td>6</td>
</tr>
<tr>
<td>3. Verifiable Parental Consent</td>
<td>6</td>
</tr>
<tr>
<td>4. Exceptions to Verifiable Parental Consent</td>
<td>8</td>
</tr>
<tr>
<td>5. Collection and Use of Third Party PI</td>
<td>14</td>
</tr>
<tr>
<td>6. Access</td>
<td>14</td>
</tr>
<tr>
<td>7. Mixed Audience Websites and Online Services</td>
<td>16</td>
</tr>
<tr>
<td>8. Promotional and Newsletter Email Communications</td>
<td>15</td>
</tr>
<tr>
<td>9. Geo-location Information</td>
<td>17</td>
</tr>
<tr>
<td>11. Photos, Video and Audio</td>
<td>18</td>
</tr>
<tr>
<td>12. Screen Names</td>
<td>18</td>
</tr>
<tr>
<td>13. Persistent Identifiers</td>
<td>18</td>
</tr>
<tr>
<td>14. Online Behavioral Advertising (OBA)</td>
<td>19</td>
</tr>
<tr>
<td>15. Material Changes</td>
<td>20</td>
</tr>
<tr>
<td>C. Data Governance</td>
<td>20</td>
</tr>
<tr>
<td>1. General Requirements</td>
<td>20</td>
</tr>
<tr>
<td>2. Data Security</td>
<td>21</td>
</tr>
<tr>
<td>3. Data Quality</td>
<td>22</td>
</tr>
<tr>
<td>4. Data Retention</td>
<td>22</td>
</tr>
<tr>
<td>5. Third Parties and Service Providers</td>
<td>22</td>
</tr>
<tr>
<td>6. Training</td>
<td>23</td>
</tr>
<tr>
<td>7. User Complaints and Feedback</td>
<td>23</td>
</tr>
<tr>
<td>8. Data Breach</td>
<td>24</td>
</tr>
<tr>
<td>D. Participant Accountability</td>
<td>24</td>
</tr>
<tr>
<td>1. Cooperation with TRUSTe</td>
<td>24</td>
</tr>
<tr>
<td>2. Annual Review</td>
<td>25</td>
</tr>
<tr>
<td>3. Certification Status</td>
<td>26</td>
</tr>
<tr>
<td>III. Definitions</td>
<td>26</td>
</tr>
</tbody>
</table>
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.

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.
II. Minimum Program Requirements

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

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:

   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;
Children’s Privacy Certification Standards

(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;

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;

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

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.

At a minimum, Participant shall link to a comprehensive Privacy Notice that discloses the Participant’s information practices.
Children’s Privacy Certification Standards

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

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

   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.

   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.
Children’s Privacy 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;
Children's Privacy Certification Standards

(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...
Children’s Privacy Certification Standards

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 parental 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
Children’s Privacy Certification Standards

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.
Children’s Privacy Certification Standards

(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.
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.
Children’s Privacy Certification Standards

being made public or sent and also Delete 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.

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 Providers** 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.
Children's Privacy Certification Standards

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

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.

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:

   (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.
Children’s Privacy Certification Standards

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

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.

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.

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)

D. Participant Accountability

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.

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

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.

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.
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.

III. Definitions

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

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.
Children’s Privacy Certification Standards

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

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.
“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.

“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.

“Third Party(ies)” is/are an entity(ies) other than the Participant or Participant’s Service Providers.

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

“Validation Page” is a web page controlled and hosted by TRUSTe that verifies the Participant’s certification status, and the TRUSTe certification scope.