



June 25, 2013

Office of the Secretary  
Room H -113  
Federal Trade Commission  
Pennsylvania Ave, NW  
Washington, DC 20580

**RE: Submission of TRUSTe's Updated Children's Privacy Program Under Section 312.11(e) of the Children's Privacy Protection Rule**

In accordance with 16 C.F.R.312.11 (e), TRUSTe submits its updated Children's Privacy Program ("Program") for approval. TRUSTe is making these updates to the Program in response to recent amendments to the Children's Online Privacy Protection Act ("COPPA"), which will become effective on July 1, 2013.

TRUSTe has operated as a COPPA safe harbor since May 2001. As of February 2013, the Program has 80 participants, representing more than 150 different online properties. We appreciate the opportunity to update our Program and believe that our amendments honor both the spirit and the letter of the new COPPA Rule.

Our submission consists of the following documents:

1. Appendix A - Children's Privacy Program Requirements
2. Appendix B - Participant Interview and Testing Checklist\*
3. Appendix C - TRUSTe's Feedback and Resolution System Dispute and Escalation Process
4. Appendix D – TRUSTe Children's Privacy Program Terms\*

The documents marked with an asterisk are considered proprietary and should be redacted from the public record.

TRUSTe believes the requirements of our Program, as implemented via our contractual infrastructure, satisfy the requirements imposed by the final COPPA Rule for assessing and monitoring the activities of COPPA Operators. We appreciate the Commission's review and approval of our submission in this regard and we look forward to continuing our role as an approved COPPA safe harbor.

For any questions regarding this submission, please contact Joanne Furtsch, Director of Product Policy, at [jfurtsch@truste.com](mailto:jfurtsch@truste.com).

Sincerely,

Tim Sullivan  
Chief Financial Officer



## Appendix A Children's Privacy Program Requirements

### I. Introduction

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.

### II. Structure

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



## Appendix A Children's Privacy Program Requirements

### III. Definitions

The following definitions shall apply herein:

- A. "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.
- B. "Child(ren)" is an (are) Individual(s) under the age of 13.
- C. "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.
- D. "Delete" means to remove PI such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.
- E. "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.
- F. "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 Program Requirements.
- G. "Foreign Language Privacy Statement" is the Participant's Privacy Statement translated into a language other than English.
- H. "Individual" means the discrete person to whom the collected information pertains.
- I. "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:



## Appendix A Children's Privacy Program Requirements

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.
- J. "Mixed Audience Website or Online Service" is an online property that is Directed to Children but Children under 13 are not the primary audience.
- K. "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.
- L. "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.
- M. "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.
- N. "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.
- O. "Parent" is a legal guardian of a Child.
- P. "Participant" means any entity that entered into an agreement with TRUSTe to participate in the TRUSTe program(s) and agreed to comply with the Program Requirements included therein and 1) has been determined to be an Operator as defined in these Program Requirements 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.



## Appendix A

### Children's Privacy Program Requirements

- Q. "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.
- R. "Privacy Statement" shall mean the statements of Participant's information collection and usage practices, as such practices are updated from time to time. Participant's Privacy Statement includes, but is not limited to:
1. A single, comprehensive statement of all the Participant's information practices ("Comprehensive Privacy Statement");
  2. A summary notice highlighting the Participant's information practices ("Short Notice"); or
  3. Disclosure of specific information practices posted at the point of information collection ("Just in Time Notice").
- S. "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.
- T. "Support for the Internal Operations" means those activities necessary to:
1. Maintain or analyze the functioning of the website or online service;



## Appendix A Children's Privacy Program Requirements

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 IV.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.

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

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

### IV. Minimum Program Requirements

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:

- A. Participant Accountability
  1. Participant shall have processes in place to comply with these Program Requirements
  2. Cooperation with TRUSTe
    - a) Provide, at no charge to TRUSTe or its representatives, full access to the Online properties (i.e., including access to premium or members only areas) for the purpose of conducting reviews to ensure that Participant's Privacy Statement(s) is consistent with actual practices.
    - b) Provide, upon TRUSTe's request, information regarding how PI gathered from and/or tracked through Participant's Online properties is used.



## Appendix A

### Children's Privacy Program Requirements

3. Annual Recertification
  - a) Participant shall undergo re-certification to verify ongoing compliance with these Program Requirements at least annually.
4. Termination for Material Breach
  - a) In the event TRUSTe reasonably believes the Participant has materially breached these Program Requirements, TRUSTe may terminate the Participant's participation in this program upon twenty (20) business days' prior written notice ("Notice of Termination") unless the breach is corrected within the same twenty (20) business day period ("Cure Period").
  - b) Material breaches of these Program Requirements include but are not limited to:
    - (1) Participant's continual, intentional, and material failure to adhere to these Program Requirements;
    - (2) Participant's material failure to permit or cooperate with a TRUSTe investigation or review of Participant's Online properties or practices pursuant to the Program Requirements;
    - (3) Participant's continual, intentional, and material failure to comply with any Suspension Obligations;
    - (4) Participant's material failure to cooperate with TRUSTe regarding an audit, complaint or the compliance monitoring activities of TRUSTe.
5. Suspension Status
  - a) In the event TRUSTe reasonably believes that Participant has materially violated these Program Requirements, Participant may be placed on Suspension.
    - (1) Notice will be provided with a mutually agreed upon description of the violation and any remedial actions that TRUSTe will require Participant to take during the Suspension Period ("Suspension Obligations").
    - (2) Participant will be considered to be on Suspension immediately upon receiving notice from TRUSTe. Suspension shall last until such time as the Participant has corrected the material breach or Program Requirements violation to TRUSTe's satisfaction, but not for a period of greater than six (6) months ("Suspension Period") unless mutually agreed by the Parties.
    - (3) Suspension Obligations may include, but are not limited to:



## Appendix A Children's Privacy Program Requirements

- (a) Compliance with additional Program Requirements;
  - (b) Cooperation with heightened compliance monitoring by TRUSTe; and
  - (c) Payment to TRUSTe of mutually agreed additional amounts as compensation for TRUSTe's additional compliance monitoring.
- (4) Participant shall comply with all Suspension Obligations.
- (5) During the Suspension Period, Participant's status may be indicated via a TRUSTe Validation webpage and/or TRUSTe may require Participant to cease using the TRUSTe trustmarks.
- (6) At the end of the Suspension Period, TRUSTe will, in its discretion, either:
- (a) Determine that Participant has complied with Participant's Suspension Obligations, thereby satisfying TRUSTe's concerns;
  - (b) Extend the Suspension Period by mutual agreement with the Participant; or
  - (c) Determine that Participant has failed to comply with Participant's Suspension Obligations and immediately terminate Participant for cause.
- B. Privacy Practices
- 1. Collection Limitation
    - a) Participant shall only collect PI from a Child if:
      - (1) The Participant has provided notice to the Parent and has obtained verifiable parental consent as described in these Program Requirements prior to the collection of PI; or
      - (2) The collection falls under an exception to verifiable parental consent as described in these Program Requirements.
    - 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



## Appendix A

### Children's Privacy Program Requirements

- a) Participant shall only use a Child's PI in accordance with their posted Privacy Statement 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 Program Requirements.

#### 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 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.



## Appendix A Children's Privacy Program Requirements

- 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 Statement;
  - (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.



## Appendix A Children's Privacy Program Requirements

- 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;



## Appendix A Children's Privacy Program Requirements

- (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 Statement.
- (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.



## Appendix A Children's Privacy Program Requirements

- (iv) Have a link to the Participant's Privacy Statement;
  - (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;



## Appendix A

### Children's Privacy Program Requirements

- (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 Statement.
  - (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;



## Appendix A Children's Privacy Program Requirements

- (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 Statement.
- (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 of 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.



## Appendix A

### Children's Privacy Program Requirements

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 Statement 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.



## Appendix A Children's Privacy Program Requirements

- d) Such mechanism or process shall confirm to the Individual inaccuracies have been corrected.
  - e) Participant's Privacy Statement 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 IV.B.4 and IV.B.3; or
    - (2) Direct the Child to content that does not involve the collection, use, or disclosure of PI.



## Appendix A

### Children's Privacy Program Requirements

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 Program Requirements.
  - 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 Statement how the Individual can request removal of publicly displayed PI.



## Appendix A

### Children's Privacy Program Requirements

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



## Appendix A

### Children's Privacy Program Requirements

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 IV.B.4.a)(7) and Section IV.B.4.a)(8) of these Program Requirements.
    - 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 OBA unless the Participant has first received verifiable parental consent.
  14. 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. Privacy Statement
1. Participant shall maintain and abide by an accurate up-to-date Privacy Statement approved by TRUSTe, in its sole discretion, that states Participant's information practices, and is in conformance with these Program Requirements including, but not limited to:



## Appendix A

### Children's Privacy Program Requirements

- a) What information is collected, either through active or passive means, including whether the Participant enables the Child to make PI publicly available; the types of entity(ies), including Service Providers, collection 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 Program Requirements;
- f) How the Individual can request access to their information as required in these Program Requirements;
- 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 statement of the procedure for exercising that right;
  - (2) Review PI collected from the Child, and a statement 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 statement of the procedure for exercising that right;
- h) What types of security measures are in place to protect collected information as required in these Program Requirements;
- i) What tracking 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;



## Appendix A

### Children's Privacy Program Requirements

- 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 Statement;
  - n) Statement of participation in the TRUSTe program and define participation scope; and
  - o) Information on how to contact TRUSTe to express concerns regarding Participant's Privacy Statement or privacy practices.
2. At a minimum, Participant shall link to a Comprehensive Privacy Statement that discloses the Participant's information practices.
3. Access to the Privacy Statement shall be Clear and Conspicuous.
4. Privacy statement must be available when the Individual first engages with the Participant, such as through an application, website homepage or landing page.
5. Privacy statement 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 Statement in effect at the time of collection unless the Parent otherwise has given verifiable parental consent to the non-conforming treatment.
7. Short Notice
- a) If Participant chooses, they may provide a Short Notice highlighting their information practices including but not limited to:
    - (1) Summary of what information is collected by the Participant and/or any Third Parties and how the Participant and/or Third Parties collect that information, either through active or passive means;
    - (2) Summary of how Participant uses collected information;
    - (3) Whether Participant shares PI with Third Parties;
    - (4) How the Individual can exercise choice and request access pursuant to these Program Requirements; and



## Appendix A Children's Privacy Program Requirements

- (5) How to contact the Participant including company name, phone number, email address or link to online form, and postal address.
  - b) Access to the Short Notice shall be Clear and Conspicuous.
  - c) Short Notice shall link to Comprehensive Privacy Statement.
    - (1) Access to the Comprehensive Privacy Statement from within the Short Notice shall be Clear and Conspicuous.
  - d) Any Short Notice shall be consistent with Comprehensive Privacy Statement.
- 8. Just in Time Notice
  - a) If Participant chooses to provide Just in Time Notice, the Just in Time Notice shall describe key collection and use details regarding the Participant's collection and use practices that are relevant to the Parent at a particular time.
  - b) Any Just in Time Notice shall be consistent with the Comprehensive Privacy Statement.
- 9. Foreign Language Privacy Statement
  - a) If Participant seeks TRUSTe certification of a Privacy Statement in a language other than English, TRUSTe shall use commercially reasonable efforts to verify that Participant's Foreign Language Privacy Statement is an accurate translation of Participant's English language Privacy Statement.
  - b) Participant shall ensure that its privacy practices are the same, and that the Foreign Language Privacy Statement provides materially the same description of Participant's privacy practices as Participant's English Language Privacy Statement.
  - c) Participant must notify TRUSTe of any Material Changes to its Foreign Language Privacy Statement and submit changes to TRUSTe for review and approval.
- D. Data Governance
  - 1. General Requirements
    - a) Participant shall implement controls and processes to manage and protect PI within its control including the ones listed in this Section IV.D.



## Appendix A

### Children's Privacy Program Requirements

- b) 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 shall take commercially reasonable steps to maintain and audit internal information technology systems within Participant's control such as:
  - (1) Regularly monitor and repair systems including servers and desktops for known vulnerabilities;
  - (2) Limit access and use of PI, or 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;
  - (3) Implement protection against phishing, spam, viruses, data loss, and malware; and
  - (4) Use reasonable encryption methods such as Secure Socket Layer for transmission 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 Statement 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.



## Appendix A

### Children's Privacy Program Requirements

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 commercially useful to carry out its business purpose, or legally required; and must disclose in their Privacy Statement its policies regarding information retention. 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 take commercially reasonable steps to evaluate 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) Understand what information the Third Party or Service Provider will be collecting from the Child or the Participant, and how that information will be used; and
    - (2) Understand 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 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 Statement.



## Appendix A Children's Privacy Program Requirements

6. 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.
  7. 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).
- E. Online Behavioral Advertising (OBA)
1. Participants engaging in OBA shall disclose the following regarding Participant's OBA Practices in its Privacy Statement:
    - a) 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;



## Appendix A Children's Privacy Program Requirements

- b) 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;
  - c) Whether PI or Third Party PI is collected by, or shared with, additional Third Parties or Service Providers for the purposes of OBA; and
  - d) How and when the Individual can exercise choice as required in this Section IV.E.
2. 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.
  - a) At a minimum, such instructions or link shall be made available in the Participant's Privacy Statement.
3. 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.
4. Participant must provide a mechanism for the Parent to review what PI the Participant has collected from the Child.
5. Participant must provide a mechanism for the Parent to withdraw consent, and to request deletion or no longer use PI collected from the Child.
6. 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;
7. 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.



# TRUSTe Children's Privacy Program

## Participant Interview & Testing Checklist

**Appendix B**

**(To be redacted from public record version.)**

Proprietary

## **Table of Contents**

<b>I. Review Information</b>	<b>3</b>
<b>II. Tests</b>	<b>3</b>
<b>III. Participant Interview Questionnaire</b>	<b>3</b>
<b>IV. Notice to parents review</b>	<b>3</b>
<b>V. Privacy statement review</b>	<b>3</b>
<b>VI. Follow up questions</b>	<b>3</b>

TRUSTe Participant Interview and Testing Checklist  
Children's Privacy Program  
**TRUSTe Proprietary Document**

**I. Review Information**

**II. Tests**

**III. Participant Interview Questionnaire**

**IV. Notice to parents review**

**V. Privacy statement review**

**VI. Follow up questions**

Additional questions for the Participant that come up during testing

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.

**TRUSTe  
Feedback and Resolution System  
Dispute and Escalation Process**

**Part 1 – Overview**

**1.1 General**

A key component of TRUSTe’s certification programs is an online third-party dispute resolution mechanism. TRUSTe will review eligible requests, claims or complaints (“Complaint”) reported by a consumer through this system about a certified TRUSTe client who has been awarded a TRUSTe seal. This review is carried out through TRUSTe’s Dispute and Escalation process (the “Process”).

**1.2 Parties to the Process**

The parties to the Process are:

- \* the Complainant - the individual complaining about misuse of information or misstatement of a privacy policy, and
- \* the Participant - the TRUSTe’s client organization that:
  - i. operates the certified web site, mobile application or other certified reported in the Complaint; and
  - ii. has agreed to comply with TRUSTe’s certification standards and participate in TRUSTe’s Dispute Process.

**1.3 Confidentiality**

TRUSTe shall maintain a written record, for a commercially reasonable time, of each Complaint filed via the Process, including correspondence exchanged through the Process and the determination for each Complaint.

**Complainant’s Consent:** Complainants are asked to indicate whether they expressly consent to sharing their report, including personally identifiable information, with the Participant that is the subject of the Complaint. The Complainant is advised that many types of reports, such as those requesting account-specific research or changes (e.g. unsubscribe requests), require such express consent so the Participant can research and respond. If the consumer does not consent to such sharing, TRUSTe staff evaluate the nature of the complaint to determine what investigation, if any, is warranted.

**Participant Responses:** Participants are advised that direct responses via the Feedback and Resolution System can be viewed by the Complainant. Participants are offered the option to notify TRUSTe if they wish to discuss the issue directly with TRUSTe (such as if they wish to discuss any confidential aspects) prior to the Participant making the required written response via the Feedback and Resolution System. The written history of the Complaint within the Feedback and Resolution System is the record of a Complaint, the issues defined, the facts presented, and the determination(s) reached by TRUSTe.

## **1.4 Enforcement due to Failure to Participate**

When TRUSTe's preliminary review of a Complaint indicates it is an eligible claim and the Participant indicates directly or indirectly that it is not willing to participate in the process, or the Participant otherwise fails to comply with the Process requirements for response or appeal after a TRUSTe decision requiring corrective action, TRUSTe shall take appropriate action. This may include Enforcement Action, such as written notice of Suspension, or written notice of Termination for Cause, if the violation is not cured within the time specified (TRUSTe may, in its sole judgment, approve an extension). Failing to cure such written notice of Enforcement Action results in Termination for Cause by TRUSTe, removal from the certification program, and revocation of the seals. Depending on the nature of the issue, TRUSTe may refer the matter to the appropriate government agency and/or publish the termination on TRUSTe's web site (e.g. TRUSTe's termination of ClassicCloseouts.com)<sup>1</sup>.

## **Part 2 - Eligible Complaints**

### **2.1 Summary**

To have a Complaint eligible for resolution through the Process, the Complainant must be personally eligible to file a Complaint and must have an eligible issue.

The Complainant must be (i) the person who provided the personal information to the organization or individual that collected it and allegedly misused it, (ii) the parent or legal guardian of the person in the case of information related to a child under 13, or (iii) the subject of the information in the case of information related to an individual that was collected online from another source.

The Complainant must have made a good faith attempt to resolve his/her Complaint directly with the Participant about whom he or she is complaining, following the procedures set out in the Participant's privacy policies.

### **2.2 Eligible Claims**

The Process is a formal written online dispute resolution mechanism.

The party registering a Complaint with TRUSTe must do so by completing the online form for TRUSTe's Feedback and Resolution System via TRUSTe's web site. In some cases, depending on the nature of the Certification, the Participant has arrangements for TRUSTe to accept Complaints via postal mail or facsimile. For issues not submitted through these authorized channels, such as complaints received via phone, voicemail, e-mail, or postal/facsimile communications (if postal/facsimile is not explicitly permitted under a certification), TRUSTe will generally attempt to instruct the individual that they

---

<sup>1</sup> One of our prior FTC referrals was Classic Closeouts in 2008; TRUSTe assisted the FTC with the investigation, and the agency brought action for permanent injunction and relief against the site, ultimately obtaining a \$2.08 million settlement to provide redress for consumers. See *Merchandise Who Illegally Charged Consumers' Accounts Settles with FTC*, available at: <http://www.ftc.gov/opa/2011/01/classicclose.shtm>

must file a written Complaint.

The Complainant must allege that the Participant used personally identifiable information about the Complainant in a manner inconsistent with Participant's published online privacy policies or otherwise violated TRUSTe's privacy certification requirements.

The Complaint must not be ineligible for one of the reasons stated below.

### **2.3 Ineligible Claims**

TRUSTe does not have authority to consider issues that fall outside the scope of TRUSTe's privacy programs. TRUSTe is not obligated to consider a claim if:

- \* the Complaint refers to activity by an uncertified web site or online property or company not subject under the applicable TRUSTe program(s);
- \* the Complainant is raising an issue on behalf of another individual for whom Complainant is not the legal guardian;
- \* the Complainant seeks only monetary damages;
- \* the Complaint alleges issues that otherwise fall outside TRUSTe's authority under its certification program(s), such as billing errors, product quality or fulfillment issues, or alleged violations of statutory or regulatory law;
- \* the Complaint refers to an issue that has been adjudicated under a previous court action, arbitration, or other form of dispute settlement;
- \* the Complainant does not consent to sharing the Complaint with the Participant to enable the Participant to research the issue and respond;
- \* the Complainant fails to respond to TRUSTe's request for clarification, documentation or other information;
- \* the issue was presented to TRUSTe via telephone, voice mail or other ineligible channel (see above).

### **2.4 Frivolous and Harassing Claims**

TRUSTe is under no obligation to pursue any complaint which TRUSTe, in its sole discretion, deems to be frivolous or to constitute harassment of TRUSTe or a Participant. A Complaint is frivolous if it has no factual basis, or if it has no basis in any obligations imposed under the applicable TRUSTe programs. Harassing complaints include successive issues based on allegations previously rejected or addressed by TRUSTe, or the filing of multiple complaints with TRUSTe employees other than those designated by TRUSTe to receive complaints.

### **2.5 Available Remedies**

A Complainant may seek to have the information that she or he submitted online, which is the subject of the Complaint, used in a manner consistent with the company's published privacy policies and, if applicable, TRUSTe's Program Requirements. A complaint also may seek to have that information corrected.

TRUSTe may require corrective action in the form of:

- \* account-specific changes, such as unsubscribing a consumer or ceasing publication of data about consumer on Participant's web site or mobile application;
- \* a change to Participant's privacy policy or practices;
- \* a third party audit if TRUSTe deems such action to be warranted.

TRUSTe, as outlined in Section 2.3 above, cannot direct corrective action that would require monetary damages or relief that would require the Participant to violate legal requirements.

## **2.6 Filing Complaints**

Filing a Complaint is the first point of contact for those who want to submit an issue for review under TRUSTe's Process.

Once a Complaint is opened via the Process, TRUSTe's system automatically assigns a ticket number to each Complaint and sends an e-mail acknowledgement. Subsequent communication is via e-mail or via an optional web interface that Complainant or Participant can use for posting updates.

TRUSTe staff reviews new Complaints within 10 business days. TRUSTe informs the Complainant if it determines that a Complaint is ineligible, or needs further information from the Complainant, or if TRUSTe is forwarding a Complaint to the Participant for response.

TRUSTe will evaluate Complaints filed to determine whether the complaint is eligible for TRUSTe review, including whether:

- \* the web site or online property is certified by TRUSTe;
- \* the Complainant has standing to file about the issue described;
- \* the Complainant is required to contact Participant directly and allow Participant to respond;
- \* the issue Complainant alleged falls outside the scope of TRUSTe's privacy certification.

If an issue is potentially eligible, then TRUSTe may determine, in its sole judgment, that additional information is required from the Complainant and/or Participant to assess eligibility, or to clarify or document information. Complainant and/or Participant shall respond within a timeframe as directed by TRUSTe.

## **2.7 Complainant's Prior Attempt to Resolve the Complaint**

TRUSTe may inquire into the nature of Complainant's attempts to resolve the issue through direct contact with the Participant, including how and when Complainant contacted the Participant and the nature response from Participant. If there was insufficient attempt to resolve the Complaint through direct contact with the Participant, TRUSTe may require the Complainant to do so and allow time for response. TRUSTe may require documentation of such attempt.

## **Part 3 - Dispute Resolution by TRUSTe**

### **3.1 Summary**

TRUSTe, in its sole judgment, shall be responsible for determining the eligibility of a Complaint and the documentation requirements, and for evaluating, investigating, analyzing and making a determination regarding the merits of an eligible Complaint.

TRUSTe's determination can vary based on factors such as the quality of the information provided by the Complainant or Participant, the verifiability of the claim, etc.

### **3.2 Duration of the Process**

After TRUSTe's system automatically acknowledges receipt and assigns a ticket number, TRUSTe conducts its initial review within 10 business days, determining whether further information is needed from the Complainant (e.g. clarification; documentation; or consent to share with Participant) and/or determining the eligibility of the issue for further research.

The duration of the investigation needed can vary widely depending on the nature of the issue or clarifications needed. TRUSTe quickly checks all issues that can be immediately verified. If our findings do not verify the Complainant's allegations, or if the issue stated falls outside the scope of TRUSTe's authority under our certification program(s), TRUSTe informs the Complainant.

The Participant is provided a timeline to provide a written response as directed by TRUSTe. For more urgent issues, such as security vulnerabilities, TRUSTe often escalates to the Participant via telephone. especially if TRUSTe has verified the problem. Certain issues, such as reproducing a leak unique e-mail address or other personal information, involve keeping a Complaint open for longer-term monitoring to try to reproduce Complainant's report.

If a Participant fails to answer a complaint with a timely response, TRUSTe will send the Participant a second notice. If the second notice and additional telephone outreach do not resolve the issue within a timeframe as directed by TRUSTe, TRUSTe may:

- \* Withdraw or suspend the Participant's use of the TRUSTe seal;
- \* Refer the matter to the appropriate government agency depending on the nature of the Complaint; and/or
- \* If Participant is terminated for cause, post a termination notice on the TRUSTe website.

TRUSTe may, in its sole discretion, extend any of the time periods discussed herein, and may elect not to consider information it receives after any specified deadline or extension of time.

TRUSTe will close an eligible Complaint when it has issued its determination, or when Complainant has failed to respond within 14 calendar days to a request for further response. When closing an eligible Complaint, TRUSTe will send its written determination and will include information in case the party or parties wish to appeal.

## **Part 4 – Appeal Process**

### **4.1 Summary**

After TRUSTe issues its determination and sends notice that it is closing an eligible Complaint, the parties are permitted to file an appeal. Notification of the right to appeal shall be posted on the TRUSTe web site.

### **4.2 Grounds for Appeal**

The Complainant or Participant in any eligible Complaint may appeal TRUSTe's determination after TRUSTe has closed the Complaint.

For example, a Complainant may file an appeal if they believe TRUSTe misunderstood an aspect of their Complaint, erred in interpreting TRUSTe program requirements, or if Complainant received new information that was not previously available.

Complaints that are not closed (e.g. still open or pending) are not eligible for appeal.

TRUSTe's determination about whether an issue falls within the scope of its authority under its certification program(s) is final, and is not subject to appeal via the Appeals Process.

### **4.3 Filing an Appeal**

Appeals must be submitted within 14 calendar days of receiving TRUSTe's e-mail notice that TRUSTe is closing the Complaint. The appeal must include their ticket number and state the grounds for appeal. The party filing the appeal must explain, in a statement not to exceed 1,000 words, why TRUSTe's final determination of the Complaint should be overturned. ("Appeal Statement").

### **4.4 Handling of the Appeal**

Upon receiving an appeal, TRUSTe's Compliance Director will review the Complaint and determine within 10 business days whether the Complaint is eligible to be reopened for further investigation. For example, TRUSTe may reopen an investigation if the Complainant reports substantive new information that a resolution a Participant indicated was applied has ceased having effect.

After TRUSTe's Compliance Director completes TRUSTe's review, TRUSTe may direct the other party to respond as directed by TRUSTe, explaining in a statement not to exceed 1,000 words why TRUSTe's final determination should be sustained, or supplying responses to specific questions from TRUSTe. The party filing the original appeal will be notified if TRUSTe is seeking response from the other party.

If TRUSTe's Compliance Director determines that the original Complaint disposition was proper according to TRUSTe processes, and introduces no substantive new information that could not have been raised earlier, or finds no other basis for appeal,

the Compliance Director will request review by TRUSTe's Legal Department of the issue appealed, and TRUSTe will respond with its final appeals determination within ten business days.

**Part 5 – Reporting of TRUSTe Complaint Activity**

TRUSTe shall publish Complaint statistics in its annual Transparency Report or other document on its web site. The reports shall provide a statistical summary of the number and categories of Complaints filed, and the number and categories of Resolutions for the Complaints, as well as the number of enforcement actions (Suspension or Termination for Cause) taken by TRUSTe. Please see pages 10-14 and Appendix D of the 2012 Transparency Report which is available online at:

[http://www.truste.com/window.php?url=http://download.truste.com/TVarsTf=A94G2B  
BP-381](http://www.truste.com/window.php?url=http://download.truste.com/TVarsTf=A94G2B<br/>BP-381)

**Appendix D**  
**TRUSTe Business Proprietary & Confidential**

TRUSTe CHILDREN'S PRIVACY PROGRAM TERMS

(To be redacted from public record version)

**Appendix D**  
**TRUSTe Business Proprietary & Confidential**

EXHIBIT A

TRUSTe MARK

# **Appendix D**

## **TRUSTe Business Proprietary & Confidential**

EXHIBIT B

CHILDREN'S PROGRAM REQUIREMENTS  
(link to program requirements posted on TRUSTe's website at [www.truste.com](http://www.truste.com))

**Appendix D**  
**TRUSTe Business Proprietary & Confidential**

EXHIBIT C

PROPERTIES TO BE CERTIFIED UNDER THIS AGREEMENT