ARISTOTLE
Now You Know™

www.aristotle.com

SALES
(800) 296-2747
sales@aristotle.com

SUPPORT
(800) 243-4401
support@aristotle.com

WASHINGTON
205 Pennsylvania Ave., SE
Washington, DC 20003
p (202) 543-8345
f (202) 543-6407

ATLANTA
1708 Peachtree St., NW
Suite 320
Atlanta, GA 30309
p (800) 296-2747
f (404) 875-5757

SAN DIEGO
3625 Ruffin Rd.
Suite 100
San Diego, CA 92123
p (858) 634-5113
f (858) 634-5111

SAN FRANCISCO
2237 Union St.
San Francisco, CA 94123
p (415) 440-1012
f (415) 440-2162

SALT LAKE CITY
775 W 1200 N Suite-200A
Springville, UT 84663
(p)(877) 580-5425
(p)(801) 609-7940

TORONTO
2255B Queen Street East
Suite #812
Toronto, Ontario M4E 1G3
Canada
p (416) 323-1961

LONDON
JGR Suite, Waverley House
7-12 Noel St.
London, W1F 8GQ
+DX 44627, Mayfair
p +44 (0)20-7339-7035
f +44 (0)20-7339-7001

June 17, 2013

Secretary of the Commission
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D. C. 20580

RE: Request for Safe Harbor Approval by the Federal Trade Commission for Aristotle International, Inc.'s Integrity Safe Harbor Compliance Program Under Section 312.11 of the Children's Online Privacy Protection Rule.

Dear Secretary:

Pursuant to the Children's Online Privacy Protection Rule ("Final Rule") (16 C.F.R. Part 312), Aristotle International, Inc. ("Aristotle") respectfully submits the following revised application for approval of the Integrity Safe Harbor Compliance Program ("Integrity Children's Privacy Compliance Program") as a safe harbor children's privacy program within the meaning of the Final Rule, Section 312.11, implementing the Children's Online Privacy Protection Act (15 U. S. C. sec. 6501 et. seq.), as amended.

Aristotle's revised safe harbor application is divided into three parts:

Part I includes a comparison of each provision of Section 312.2 through Section 312.10 with the corresponding provisions of the Program Requirements;

Part II includes the full text of the revised Integrity Children's Privacy Compliance Program Requirements ("Program Requirements"), modified to comply with the Final Rule, as amended.

Part III includes the following documents (those documents marked with a double asterisk are proprietary and are to be redacted from the public record version):

Exhibit 1: Integrity Children's Privacy Compliance Program Membership Agreement** (proprietary)

Exhibit A to Membership Agreement: Program Requirements (public)

Appendix 1 to Program Requirements: Verification Page (public)

www.aristotle.com

SALES
(800) 296-2747
sales@aristotle.com

SUPPORT
(800) 243-4401
support@aristotle.com

WASHINGTON
205 Pennsylvania Ave., SE
Washington, DC 20003
p (202) 543-8345
f (202) 543-6407

ATLANTA
1708 Peachtree St., NW
Suite 320
Atlanta, GA 30309
p (800) 296-2747
f (404) 875-5757

SAN DIEGO
3625 Ruffin Rd.
Suite 100
San Diego, CA 92123
p (858) 634-5113
f (858) 634-5111

SAN FRANCISCO
2237 Union St.
San Francisco, CA 94123
p (415) 440-1012
f (415) 440-2162

SALT LAKE CITY
775 W 1200 N Suite-200A
Springville, UT 84663
(p)(877) 580-5425
(p)(801) 609-7940

TORONTO
2255B Queen Street East
Suite #812
Toronto, Ontario M4E 1G3
Canada
p (416) 323-1961

LONDON
JGR Suite, Waverley House
7-12 Noel St.
London, W1F 8GQ
+DX 44627, Mayfair
p +44 (0)20-7339-7035
f +44 (0)20-7339-7001

Appendix 2 to Program Requirements: Self-Evaluation Form** (proprietary)

Exhibit B to Membership Agreement: Sample Marks (public)

Exhibit 2: Monitoring Review Report Form** (proprietary)

Thank you very much,

J. Blair Richardson

Aristotle International

General Counsel and Chief Privacy Officer

Integrity Children's Privacy Compliance Program

Part I.

A COMPARISON OF EACH PROVISION OF SECTION 312.2 THROUGH SECTION 312.10 WITH THE CORRESPONDING PROVISIONS OF THE CHILDREN'S PRIVACY COMPLIANCE PROGRAM REQUIREMENTS. (Formerly Part II of February 15, 2012 Revised Request for Safe Harbor Approval by the Federal Trade Commission for Aristotle International, Inc.'s Integrity Safe Harbor Compliance Program Under Section 312.10 of the Children's Online Privacy Protection Rule.)

Version No: 2.5
Last Updated: June 25, 2013

Section 312.2 ***Definitions***

Corresponding Section of the Children's Privacy Compliance Program Requirements:

The definitions in Section 312.2 have been added to the Children's Privacy Compliance Program Requirements, as well as being incorporated by reference into the Integrity Children's Privacy Compliance Program Membership Agreement.

Section 312.3: *Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.*

Corresponding Section of the Children's Privacy Compliance Program Requirements:

Under sec. 312.3, the Final Rule sets forth the overall scheme of the COPPA, which is to regulate unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. Specifically, the Final Rule states under sec. 312.3 that an operator must:

- Provide notice on the website or online service of what information it collects from children, how it uses such information, and disclosure practices for such information;
- Obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children;
- Provide a reasonable means for a parent to review the personal information collected from a child, delete it and to refuse to permit its further use or maintenance;
- Not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and,
- Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

Under the Children's Privacy Compliance Program, member companies are required to adhere to and abide by this general requirement in order to prevent any possibility of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. Specifically, member companies must comply with the following seven program requirements:

Requirement 1 (Notice/Disclosure of Information): Member companies must post a prominent link that is clearly labeled Privacy Policy or such similar notice that links the parent or child to a description of the member's information collection, use, and disclosure practices.

Requirement 2 (Direct Notice to Parents): Member companies must make reasonable efforts to ensure that a parent of a child receives notice of the Member's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent had previously consented.

Requirement 3 (Prior Verifiable Parental Consent): Members must obtain verifiable consent before any collection, use, display or disclosure of personal information from children or a persistent identifier unless permitted to collect the child's name, online contact information, or a persistent identifier under one of the exceptions to prior verifiable parental consent set forth in sec. 312.5 (c) the Final Rule.

Requirement 4 (Access and Review): Member companies must provide parents with the ability to access and review their child's personal information, to delete it, and to refuse to permit its further use or maintenance.

Requirement 5 (Restrictions on Information Collection): Member companies must not condition a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

Requirement 6 (Confidentiality, Security and Integrity of Information): Member companies must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

Requirement 7 (Compliance and Enforcement): Member companies must implement effective and meaningful compliance and enforcement mechanisms that ensure that they comply with their information policies and practices.

Section 312.4: *Notice*.

Corresponding Sections of the Children's Privacy Compliance Program Requirements:

Requirement 1: Notice/Disclosure of Information

Members that collect personal information from children must post a prominent link that is clearly labeled *Privacy Policy* or such similar notice that links the children to a description of the Member's information collection, use, and disclosure practices.

The privacy policy link must be plainly visible on the home or landing screen or page and in close proximity to any area where children directly provide, or are asked to provide, Personal Information. If the Site has a separate children's area, Member must also provide a link to the Privacy Policy in a clear and prominent place and manner on the home or landing screen or page of that area. The link at each such location must clearly indicate that the Privacy Policy includes information about the Site's information practices with regard to children.

Privacy Policies must be clear and understandable, and should not contain unrelated, contradictory, promotional or confusing material. The privacy policies must be reconciled with Terms of Use, Terms of Service or End User License Agreement, so that activities on a site and all posted policies are consistent.

Privacy Policies must describe the following information:

A. Notice of last update: Members must include a notice at the top of the privacy policy clearly stating when it was last updated.

B. Member Contact Information: Members must include their complete contact information. Such information must include the name, physical address, telephone number, and email address of all operators collecting or maintaining personal information from children through the website or online service. Members may list the name, address, phone number, and e-mail address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the website or online service are also listed in the notice.

C. Types of Personal Information Collected: Members must describe what information any operator collects from children, including whether the website or online service enables a child to make personal information publicly available, and whether the personal information is collected directly or passively.

D. Use of Personal Information: Members must describe how personal information is used.

E. Disclosure of Personal Information: Members must state whether personal information is disclosed to third parties. If the Member does disclose personal information, the Member must: (1) describe the types of business in

which such third parties are engaged and the general purposes for which the information is used; (2) state that the third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the Member; and (3) state that the parent has the option to consent to the collection and use of their child's personal information without consenting to the disclosure of that information to third parties.

F. Control Over Personal Information: Members must state in their privacy policies the choices available to the parent and the child regarding how the child's personal information is collected and used.

G. Access to Information, Deletion, Refusal to Permit Further Collection or Use: Members must state that parents can review the child's personal information, have such information deleted, and refuse to permit further collection or use of the child's information. Members must also indicate the procedures that the parent must follow for doing so.

H. Data Security and Protection: Members must state that a) they have established and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children; and b) they take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

I. Questions/Complaints: Members must state in their privacy policies where the parent or child can address any questions or complaints that they may have about the website information practices. Members must include the information on how to submit complaints about the Member's websites directly to the Children's Privacy Compliance Program.

Requirement 2: Direct Notice to Parents

A Member must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the operator's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented.

Requirement 2 sets forth the specific types of information that must be contained in the following types of Direct Notices to Parents:

A. *Notice to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information*.

B. *Voluntary Notice to Parent of a Child's Online Activities Not Involving the Collection, Use or Disclosure of Personal Information.*

C. *Notice to a Parent of Operator's Intent to Communicate with the Child Multiple Times.*

D. *Notice to a Parent In Order to Protect a Child's Safety*.

Section 312.5: *Parental consent.*

Corresponding Section of the Children's Privacy Compliance Program Requirements:

Requirement 3: Prior Verifiable Parental Consent

A. Generally: Subject to the exceptions set out in this Requirement, Members must obtain verifiable parental consent before any collection, use, or disclosure of personal information from children. Members must also obtain such consent to any material change in the collection, use, or disclosure practices to which the parent has

previously consented. Members must give parents the option to consent to the collection and use of the child's personal information without consenting to disclosure of that information to third parties.

B. Method for Obtaining Verifiable Parental Consent: To comply with Requirement 3 (Prior Verifiable Parental Consent), Members must obtain prior verifiable parental consent. Any method to obtain prior verifiable parental consent must be reasonably calculated, in light of the available technology, to ensure that the person providing consent is the child's parent.

Methods to obtain prior verifiable parental consent include: (i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan; (ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder; (iii) Having a parent call a toll-free telephone number staffed by trained personnel; (iv) Having a parent connect to trained personnel via video-conference; (v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; or (vi) using the Integrity System as described in Requirement 3(B).

C. Where Member Does Not Disclose Children's Personal Information

A member operator that does not "disclose" children's personal information, may use email coupled with additional steps to provide assurances that the person providing the consent is the parent.

D. Exceptions to Verifiable Parental Consent: The exceptions to prior verifiable parental consent are where the sole purpose of collecting the information from the child is: i) to provide notice and obtain parental consent to the Collection, Use, or Disclosure of a Child's Personal Information; ii) to provide voluntary notice to, and subsequently update the parent about, the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information; iii) to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request; iv) to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child; v) to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety; vi) to protect the security or integrity of the website or online service, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or for investigations on matters related to public safety, so long as the information is not used for any other purpose; vii) where a Member collects a persistent identifier and no other personal information, and such identifier is used for the sole purpose of providing support for the internal operations of the website or online service; and viii) where an operator covered under paragraph (b) of the definition of *website or online service directed to children* collects a persistent identifier and no other personal information from a user who affirmatively interacts with the operator and whose previous registration with that operator indicates that such user is not a child.

Section 312.6: *Right of parent to review personal information provided by a child.*

Corresponding Section of the Children's Privacy Compliance Program Requirements:

Requirement 4: Access and Review

Members must provide parents with the ability to access and review their child's personal information. Upon request of a parent whose child has provided personal information to a Member, the Member is required to provide to that parent the following:(1) A description of the specific types or categories of personal information collected from children by the Member, such as name, address, telephone number, e-mail address, hobbies, and extracurricular activities;(2) The opportunity at any time to refuse to permit the Member's further use or future online collection of personal information from that child, and to direct the Member to delete the child's personal

information; and(3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the Member to carry out this provision must: (i) Ensure that the requestor is a parent of that child, taking into account available technology; and (ii) Not be unduly burdensome to the parent.

Section 312.7: *Prohibition against conditioning a child's participation on collection of personal information*.

Corresponding Section of the Children's Privacy Compliance Program Requirements:

Requirement 5: Restrictions on Information Collection

A child-directed site may not use an age gate.

The age information on the registration form of a site that is not child-directed or where children are not the primary audience must be asked in a neutral manner that does not invite falsification. Members must employ temporary or permanent cookies to prevent children from back-buttoning to change their age in order to circumvent the parental consent requirement or obtain access to the site**.**

Members are prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

Section 312.8: *Confidentiality, security, and integrity of personal information collected from children*.

Corresponding Section of the Children's Privacy Compliance Program Requirements:

Requirement 6: Confidentiality, Security and Integrity of Information

Members must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The Member must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

Section 312.10: *Data retention and deletion requirements.*

Corresponding Section of the Children's Privacy Compliance Program Requirements:

Requirement 6: Confidentiality, Security and Integrity of Information

A Member shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The Member must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

Section 312.9: *Enforcement.*

Corresponding Section of the Children's Privacy Compliance Program Requirements:

Requirement 7: Compliance and Enforcement

Members must implement effective and meaningful compliance and enforcement mechanisms that ensure that they comply with their information policies and practices, including:

A. Appointment of a Program Representative.
B. Initial and annual self-evaluation.
C. Submitting to compliance monitoring.
D. Providing the parent and the child with reasonable and effective means to submit complaints.
E. Executing the Children's Privacy Compliance Program membership agreement, which includes agreement to comply with the Program Requirements at all times.
F. Agreeing to referral to Governmental Agencies for failure to comply with Membership Agreement.
G. Members being provided detailed reports on results of audits, disciplinary actions and consumer complaints.

Integrity Children's Privacy Compliance Program

INTEGRITY CHILDREN'S PRIVACY COMPLIANCE PROGRAM REQUIREMENTS

Version No: 2.5
Last Updated: June 25, 2013

To help facilitate a safe and secure environment for children online, Aristotle offers seven requirements as guidelines that Member companies must follow when operating websites directed in whole or in part to children 12 years old and under that collect information from children, or that have actual knowledge they collect information from children 12 years old and under.

Aristotle's Program Requirements will be modified as necessary to meet the requirements of the Children's Online Privacy Protection Act (COPPA) and its implementing Rule, 16 C.F.R. Part 312. Aristotle's Children's Program has been approved by the Federal Trade Commission as an authorized safe harbor under the COPPA rule. All Members are required to meet the requirements of the Program and the COPPA rule. Members will have the option of contracting for Aristotle to administer their programs for individual notice and consent, common consent, and/or parental access and review.

Definitions

Child means an individual under the age of 13.

Children means individuals under the age of 13.

Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:

(a) Requesting, prompting, or encouraging a child to submit personal information online;

(b) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or

(c) Passive tracking of a child online.

Commission means the Federal Trade Commission.

Delete means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

Disclose or disclosure means, with respect to personal information:

(a) The release of personal information 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

(b) Making personal information 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.

Internet means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

Online contact information means an email 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.

Operator means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of 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 involving commerce:

(a) Among the several States or with 1 or more foreign nations;
(b) In any territory of the United States or in the District of Columbia, or between any such territory and
(1) Another such territory, or
(2) Any State or foreign nation; or
(c) Between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

Personal information is *collected or maintained on behalf of* an operator when: (a) it is collected or maintained by an agent or service provider of the operator; or (b) the operator benefits by allowing another person to collect personal information directly from users of such website or online service.

Parent includes a legal guardian.

Person means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

Personal information means individually identifiable information about an individual collected online, including:

(a) A first and last name;
(b) A home or other physical address including street name and name of a city or town;
(c) Online contact information as defined in this section;
(d) A screen or user name where it functions in the same manner as online contact information, as defined in this section;
(e) A telephone number;
(f) A Social Security number;
(g) 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;
(h) A photograph, video, or audio file where such file contains a child's image or voice;
(i) Geolocation information sufficient to identify street name and name of a city or town; or
(j) 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.

Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.

Support for the internal operations of the website or online service means those activities necessary to:

(a) maintain or analyze the functioning of the website or online service;
(b) perform network communications;
(c) authenticate users of, or personalize the content on, the website or online service;
(d) serve contextual advertising on the website or online service or cap the frequency of advertising;
(e) protect the security or integrity of the user, website, or online service;
(f) ensure legal or regulatory compliance; or
(g) fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4) of the COPPA Rule, in accordance with Requirement 3 D of the Program Requirements;

so long as the information collected for the activities listed in paragraphs (a)-(g) is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose.

Third party means any person who is not:

(a) An operator with respect to the collection or maintenance of personal information on the website or online service; or
(b) A person who provides support for the internal operations of the website or online service and who does not use or disclose information protected under this part for any other purpose.

Obtaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

(a) Receives notice of the operator's personal information collection, use, and disclosure practices; and
(b) Authorizes any collection, use, and/or disclosure of the personal information.

Website or online service directed to children means a commercial website or online service, or portion thereof, that is targeted to children:

(a) In determining whether a website or online service, or a portion thereof, is directed to children, the Commission will consider its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.

(b) A website or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another website or online service directed to children.

(c) A website or online service that is directed to children under the criteria set forth in (a) above, but that does not target children as its primary audience, shall not be deemed directed to children if it: (i) does not collect personal information from any visitor prior to collecting age information; and (ii) prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of this part.

(d) A website or online service shall not be deemed directed to children solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

Requirement 1: <u>Notice/Disclosure of Information</u>

Members who are operators of any website or online service directed to children, or who have actual knowledge that their website or online service is collecting or maintaining personal information from children, must post a prominent link that is clearly labeled "Privacy Policy" or such similar notice that links the children to a description of the Member's information collection, use and disclosure practices, may display the Children's Mark and must abide by these requirements as set forth herein. For any section of Member's Site that is directed at children, Member may display Aristotle's Children's Mark on such section(s) of the Site, and on no other sections, and must abide by these Program Requirements.

Members must notify the Children's Privacy Compliance Program if their online information practices change or when there are planned changes to the Member's privacy policy. The Children's Privacy Compliance Program must review and approve these changes prior to any implementations of changes.

The Privacy Policy shall be displayed as follows:

i. The Site must provide a link to the Privacy Policy in a clear and prominent place and manner on: a) Member's home or landing screen or page; and b) in close proximity to any area where children directly provide, or are asked to provide, Personal Information. If the Site has a separate children's area, Member must also provide a link to the Privacy Policy in a clear and prominent place and manner on the home or landing screen or page of that area. The link at each such location must clearly indicate that the Privacy Policy includes information about the Site's information practices with regard to children.

ii. The Privacy Policy must reside on Member's server (or that of a third party with whom Member has contracted for use of a server for the Site) unless otherwise agreed to in writing or email by Aristotle and Member. Member must provide Aristotle with the URL(s) of any Privacy Policy and must provide Aristotle written or electronic notice two (2) business days prior to changing the URL(s) of any Privacy Policy.

iii. Member may label the link to the Privacy Policy with the Aristotle mark listed in Section 2 of the Membership Agreement (Children's Mark) or a hypertext link or button with the phrase "Privacy Policy." The Children's Mark or the hypertext link must link directly to the Site's Privacy Policy.

iv. The Aristotle Mark(s) listed in Section 2 of the Agreement **(**Children's Mark), hypertext link or button must link directly to the Site's Privacy Policy.

v. The Verify Mark may be located at the top of the Privacy Policy, in either margin. The Verify Mark must link to Member's Verification Page (in the form of Appendix 1 hereto) located on Aristotle's secure server at the Aristotle website. The verification page will confirm the Site's participation in the Aristotle Program.

Aristotle will assist in drafting or modifying privacy policies. Privacy Policies must be clear and understandable, and should not contain unrelated, promotional, contradictory, or confusing material. The privacy policies must be reconciled with Terms of Use, Terms of Service or End User License Agreement, so that activities on a site and all posted policies are consistent. Privacy Policies must describe the following information:

A. Notice of last update: Members must include a notice at the top of the privacy policy clearly stating when it was last updated.

B. Member Contact Information: Members must include their complete contact information. Such information must include the name, physical address, telephone number, and email address of all operators collecting or maintaining personal information from children through the website or online service. Members may list the name, address, phone number, and e-mail address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the website or online service are also listed in the notice;

C. Types of Personal Information Collected: Members must describe what information all Operators on the Member's site collect from children, including whether the website or online service enables a child to make personal information publicly available, and whether the personal information is collected directly or passively.

D. Use of Personal Information: Members must describe how personal information is used.

E. Disclosure of Personal Information: Members must state whether personal information is disclosed to third parties. If the Member does disclose personal information, the Member must: (1) describe the types of business in which such third parties are engaged and the general purposes for which the information is used; (2) state that the third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the Member; and (3) state that the parent has the option to consent to the collection and use of their child's personal information without consenting to the disclosure of that information to third parties.

F. Control Over Personal Information: Members must state in their privacy policies the choices available to the parent and the child regarding how the child's personal information is collected and used.

G. Access to Information, Deletion, and Refusal to Permit Further Collection or Use: Members must state that parents can review the child's personal information, have such information deleted, and refuse to permit further collection or use of the child's information. Members must also indicate the procedures that the parent must follow for doing so.

H. Data Security and Protection: Members must state a) that they have established and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children; and b) that they take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

I. Questions/Complaints: Members must state in their privacy policies where the parent or child can address any questions or complaints that they may have about the website information practices. Members must include the information on how to submit complaints about the Member's websites directly to the Children's Privacy Compliance Program.

Requirement 2: <u>Direct Notice to Parents</u>

A Member must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the Member's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented. The notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials.

Direct Notices to Parents must therefore contain the following information:

A. *Notice to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information*.

This direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child, and, if such is the case, the name of the child or the parent, in order to obtain the parent's consent;
(ii) That the parent's consent is required for the collection, use, or disclosure of such information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;
(iii) The additional items of personal information the operator intends to collect from the child, or the potential opportunities for the disclosure of personal information, should the parent provide consent;
(iv) A hyperlink to the Member's Privacy Policy;
(v) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and
(vi) That if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records.

B. *Voluntary Notice to Parent of a Child's Online Activities Not Involving the Collection, Use or Disclosure of Personal Information.*

Where an operator chooses to notify a parent of a child's participation in a website or online service, and where such site or service does not collect any personal information other than the parent's online contact information, the direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child in order to provide notice to, and subsequently update the parent about, a child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information;
(ii) That the parent's online contact information will not be used or disclosed for any other purpose;
(iii) That the parent may refuse to permit the child's participation in the website or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and
(iv) A hyperlink to the Member's Privacy Policy.

C. *Notice to a Parent of Operator's Intent to Communicate with the Child Multiple Times.*

This direct notice shall set forth:

(i) That the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child;
(ii) That the operator 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 from the operator;
(iii) That the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child;
(iv) That 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) That if the parent fails to respond to this direct notice, the operator may use the online contact information collected from the child for the purpose stated in the direct notice; and
(vi) A hyperlink to the Member's Privacy Policy.

D. *Notice to a Parent In Order to Protect a Child's Safety*.

This direct notice shall set forth:

(i) That the operator has collected the name and the online contact information of the child and the parent in order to protect the safety of a child;
(ii) That the information will not be used or disclosed for any purpose unrelated to the child's safety;
(iii) That the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so;
(iv) That if the parent fails to respond to this direct notice, the operator may use the information for the purpose stated in the direct notice; and
(v) A hyperlink to the Member's Privacy Policy.

Requirement 3: <u>Prior Verifiable Parental Consent</u>

A. <u>Generally</u>: Except as provided in Sections 3(C) and 3(D), Members must obtain verifiable parental consent before any collection, use, display, or disclosure of personal information from children, and will make best efforts to prevent a child from making such information public without such consent. This includes, but is not limited to, public posting through the Internet, a home page of a website, a pen pal service, an electronic mail service, a message board, or a chat room.

Members must also obtain such consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented. Changes are material under this subsection if they relate to Member's practices regarding collection, use, or disclosure of Personal Information; notice and disclosure regarding those practices; user choice and consent regarding how Personal Information is used and shared; or measures for data security, integrity, or access. If Member materially changes its privacy practices, Member must follow Requirements 2 and 3 and provide notice and obtain verifiable parental consent before collecting, using, or disclosing Personal Information from children for the new practices. Members must notify the Children's Privacy Compliance Program when making material changes to their Privacy Policy, and may be subject to a revision fee.

Members must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.

Member shall notify Aristotle prior to (i) any Assignment or Transfer which involves sharing Personal Information between the parties; (ii) change in name of Member or (iii) change of domain name for the Site. An Assignment or Transfer of Personal Information shall be treated as a transfer to a third party of Personal Information collected by Member, and the Member must follow Requirement 2 with regard to providing parental notice and choice. Alternatively, with the prior written consent of Aristotle, which consent shall not be unreasonably withheld or delayed, Member may post prominent notices on the Site about the Assignment or Transfer provided such notices are posted for at least thirty (30) consecutive business days prior to completion of the Assignment or Transfer, where notice and verifiable parental consent are not required. If Member ceases to exist or is not the controlling entity as a result of a merger, acquisition or other organizational change, the successor of the company must meet Aristotle criteria in order to carry any Aristotle Mark(s).

B. <u>Method for Obtaining Verifiable Parental Consent</u>: To comply with Requirement 3 (Verifiable Parental Consent), Members must obtain prior verifiable parental consent. Any method to obtain prior verifiable parental consent must be reasonably calculated, in light of the available technology, to ensure that the person providing consent is the child's parent. Methods to obtain prior verifiable parental consent include: i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan; (ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder; (iii) Having a parent call a toll-free telephone number staffed by trained personnel; (iv) Having a parent connect to trained personnel via video-conference; (v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information; or (vi) using the Integrity System, a suite of online and offline methods by which an individual can authenticate his or her identity and therefore activate an account in order to provide member sites with notice and verifiable consent. The Integrity System provides a total of thirteen (13) methods of verification. The eleven online mechanisms include: (i) the verification of the last four digits of the individual's social security number; (ii) verification of the individual's driver license number; (iii) in connection with a monetary transaction, the use of a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder; (iv) email

with an electronically signed parental consent form, and verification of an attached photo, scan or copy of a form of government-issued identification (e.g., voter registration card, driver's license, other official license), where the parent's identification is deleted by the operator from its records promptly after such verification is complete; (v) email with an attached photo, scan or electronic copy (e.g., pdf format) of a physically signed parental consent form; (vi) the electronic submission through a secure website (upload) and verification of an attached photo, scan or copy of form of government-issued identification, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; (vii) the electronic submission through a secure website (upload) and verification of an attached photo, scan or copy of a physically signed parental consent form; (viii) electronic transmission and verification of a photo, scan or copy of a form of government-issued identification through Multimedia Messaging Service ("MMS"), where the parent's identification is deleted by the operator from its records promptly after such verification is complete; (ix) electronic transmission and verification of a photo, scan or copy of a physically signed parental consent form through Multimedia Messaging Service ("MMS"); (x) submission of the full name, birth date, and location of the parent, and government-issued identification number (SSN4, Driver's License Number, Passport Number, State ID Number) verified through the use of a commercially available database or aggregate of databases, consisting primarily of data from government sources, that are regularly used by government and businesses for the purpose of age and identity verification and authentication, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; and (xi) face-to-face real-time verification through online telephony or videoconferencing technology. The two offline methods include (i) printing out a parental consent form, signing it, and mailing or faxing the form to the Children's Privacy Compliance Program, and (ii) providing consent over the telephone using a toll-free number staffed by trained operators.

Integrity may approve additional methods of obtaining Verifiable Parental Consent for Members that are reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.

The Integrity system may collect personal information as part of the Prior Verifiable Parental Consent process. Secure handling and storage of such information is of the utmost and highest concern. All Personal Information submitted to Integrity, and the transaction ID number assigned to each verification request shall be stored on separate servers and separate databases independent of all other corporate data, stored in a secure encrypted form immediately after submission, and the parent's identification shall be deleted as indicated above.

All transmissions of data are in a secure communication protocol. We maintain physical, electronic and procedural safeguards to protect Personal Information that meet or exceed industry standards, and following completion of the verification transaction, the stored data shall be used only for auditing purposes pertaining to the accuracy of the verification and for no other use.

C. Where Member Does Not Disclose Children's Personal Information: A member operator that does not "disclose" children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email.

D. Exceptions to Verifiable Parental Consent: The exceptions to prior verifiable parental consent are as follows:

- *Required Parental Consent* - Where the sole purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent to the Collection, Use, or Disclosure of a Child's Personal Information under Requirement 2(A). If the Member has not obtained parental consent after a reasonable time from the date of the information collection, the Member must delete such information from its records.

- *Voluntary Notice Under Requirement 2(B)* - Where the purpose of collecting a parent's online contact information is to provide voluntary notice to, and subsequently update the parent about, the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the Member must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in Requirement 2(B).

- *One-Time Request* –Where the sole purpose of collecting online contact information from a child is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact

the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request.

- *Multiple Requests* – Where the purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the Member must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in Requirement 2(C). A Member 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.

- *Child Safety* - Where the purpose of collecting a child's and a parent's name and online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the Member must make reasonable efforts, taking into consideration available technology, to provide a parent with notice as described in Requirement 2(D).

- *Additional Safety Concerns* - Members may collect a child's first name or online contact information to protect the security or integrity of the website or online service, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or for investigations on matters related to public safety, so long as the information is not used for any other purpose. Direct notice is not required under this exception.

- *Persistent Identifier Used Solely in Support of Internal Operations* – Where a persistent identifier and no other personal information is collected and such identifier is used for the sole purpose of providing support for the internal operations of the website or online service. In such case, there also shall be no obligation to provide notice.

- *Certain Conditions Where Member Covered Under Paragraph (b) of the Definition of Website or Online Service Directed to Children Collects a Persistent Identifier* - Where a Member covered under paragraph (b) of the definition of *website or online service directed to children* collects a persistent identifier and no other personal information from a user who affirmatively interacts with the Member and whose previous registration with that Member indicates that such user is not a child. In such case, there also shall be no obligation to provide notice under § 312.4.

Requirement 4: <u>Access and Review</u>

Members must provide parents with the ability to access and review their child's personal information.

(a) Upon request of a parent whose child has provided personal information to a Member, the Member is required to provide to that parent the following:

(1) A description of the specific types or categories of personal information collected from children by the Member, such as name, address, telephone number, e-mail address, hobbies, and extracurricular activities;

(2) The opportunity at any time to refuse to permit the Member's further use or future online collection of personal information from that child, and to direct the Member to delete the child's personal information; and

(3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the Member to carry out this provision must:

(i) Ensure that the requestor is a parent of that child, taking into account available technology; and

(ii) Not be unduly burdensome to the parent.

(b) Neither a Member nor the Member's agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section.

(c) Subject to the limitations set forth in Requirement 5, a Member may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the Member's further use or collection of personal information from his or her child or has directed the Member to delete the child's personal information.

Requirement 5: Restrictions on Information Collection

A child-directed site may not use an age gate.

The age information on the registration form of a site not directed to children or where children are not the primary audience must be asked in a neutral manner that does not invite falsification. Members must employ temporary or permanent cookies to prevent children from back-buttoning to change their age in order to circumvent the parental consent requirement or obtain access to the site**.**

Members are prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

Requirement 6: Confidentiality, Security and Integrity of Information

A Member shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The Member must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

The Member must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The Member must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.
If Member collects, uses, discloses or distributes sensitive information, such as credit card numbers or social security numbers, it shall utilize appropriate commercially reasonable practices, such as encryption, to protect information transmitted over the Internet

Requirement 7: Compliance/Enforcement

A. Program Representative: Members must appoint a program representative for the website(s). The program representative shall be the individual responsible for overseeing the website compliance with the Children's Privacy Compliance Program. The program representative shall be given the authority to investigate all inquiries concerning the website's privacy policy and information practices and in a timely manner. Aristotle agrees to name an account manager for Member within fifteen (15) business days of the Effective Date by providing written or electronic notice to Member. All notices between Aristotle and Member shall be directed to the designated Program Representative and designated Aristotle account manager, which either party may change upon written or electronic notice to the other.

B. Initial and Annual Self-Evaluation: Members must conduct an evaluation of their website information collection, use, and disclosure practices. Each Member will be required to complete and attest to the accuracy of the statements they make on a Self-Evaluation form (Appendix 2 to these Program Requirements] about their information practices. Once Aristotle receives the Self-Evaluation form, an Aristotle representative will independently review the website's posted privacy policy, information practices, and the Self-Evaluation form for compliance with the Program Requirements. Once the Member website is determined to be in full compliance with the Program Requirements, it will then be listed as a Member participating in the Children's Privacy Compliance Program. Members are required to complete a Self-Evaluation form on an annual basis to ensure that their websites' information practices are consistent with their posted privacy policies and the Program Requirements.

C. Compliance Monitoring: Members must submit to monitoring of their website information practices. The purpose of monitoring reviews is to ensure that a Member's privacy policy is consistent with its website information practices. Monitoring reviews also allow the Children's Privacy Compliance Program or an independent third party designated by the Children's Privacy Compliance Program to verify that the Member's website complies with the Program Requirements at all times. The compliance monitoring may be conducted on a quarterly basis, but in no event less than annually. In addition to such monitoring, Members must also agree to submit to periodic, unannounced reviews of their websites. These unannounced reviews will be used to further verify that the Member remains in full compliance with the Program Requirements.

If the Children's Privacy Compliance Program determines that a violation of the requirements has occurred the Member is informed of such violation and the corrective actions that must be taken to bring the Member's website into compliance. Failure to take the corrective actions can result in a number of consequences including removal from the Children's Privacy Compliance Program and referral to the appropriate governmental agency.

D. Consumer Complaints/Monitoring: Members must provide the parent and the child with reasonable and effective means to submit complaints that they may have about the Member's information practices. The Children's Privacy Compliance Program also offers the parent and the child the opportunity to submit complaints about any Member directly to Aristotle's Dispute Resolution Process. A Children's Privacy Compliance Program representative responds to all complaints immediately. Members must agree to work with Aristotle representatives in their efforts to resolve all complaints that are submitted to the Children's Privacy Compliance Program Dispute Resolution Process. If Member has materially breached this Agreement, Member agrees to reimburse Aristotle for the reasonable cost of any such review and promptly rectify the practice to the Children's Privacy Compliance Program's reasonable satisfaction. Members must maintain records for a period of three (3) years of all complaints, concerns, or inquiries received about its website and any responses to the consumer addressing such complaint or concern.

E. Membership Agreement: Members must execute the Children's Privacy Compliance Program membership agreement. As part of this agreement, Members agree to comply with the Program Requirements at all times. In the event that a Member fails to meet any of its obligations under the membership agreement, such actions would constitute a material breach of the agreement and its membership in the Children's Privacy Compliance Program would be terminated.

F. Investigations/Referral to Governmental Agencies: If the Children's Privacy Compliance Program's determines, after a thorough investigation into the Member information practices that a Member has violated its posted privacy policy or any of the requirements described above, the Children's Privacy Compliance Program's may refer such Member to the Federal Trade Commission for possible unfair and deceptive trade practices.

G. Reporting Requirements: Members are provided detailed reports on results of audits, disciplinary actions and consumer complaints. Aristotle maintains a record of the results of audits, disciplinary actions and consumer complaints for a period of at least three (3) years and is made available to the member company.

Integrity Children's Privacy Compliance Program

Part III.

Exhibit 1: Integrity Children's Privacy Compliance Program Membership Agreement (Redacted from public version)

- **Exhibit A to Membership Agreement: Program Requirements**
  - **Appendix 1 to Program Requirements: Verification Page**
  - **Appendix 2 to Program Requirements: Self-Evaluation Form (Redacted from public version)**
- **Exhibit B to Membership Agreement: Sample Marks**

Exhibit 2: Monitoring Review Report Form (Redacted from public version)

Integrity Children's Privacy Compliance Program

Exhibit 1 to Request for Safe Harbor Approval by the Federal Trade Commission for Aristotle International, Inc.'s Integrity Safe Harbor Compliance Program Under Section 312.10 of the Children's Online Privacy Protection Rule.

Integrity Children's Privacy Compliance Program Membership Agreement

(Redacted From Public Record Version)

Version No: 2.4
Last Updated: June 11, 2013

Integrity Children's Privacy Compliance Program

Exhibit A to Membership Agreement

INTEGRITY CHILDREN'S PRIVACY COMPLIANCE PROGRAM REQUIREMENTS

Version No: 2.5
Last Updated: June 25, 2013

To help facilitate a safe and secure environment for children online, Aristotle offers seven requirements as guidelines that Member companies must follow when operating websites directed in whole or in part to children 12 years old and under that collect information from children, or that have actual knowledge they collect information from children 12 years old and under.

Aristotle's Program Requirements will be modified as necessary to meet the requirements of the Children's Online Privacy Protection Act (COPPA) and its implementing Rule, 16 C.F.R. Part 312. Aristotle's Children's Program has been approved by the Federal Trade Commission as an authorized safe harbor under the COPPA rule. All Members are required to meet the requirements of the Program and the COPPA rule. Members will have the option of contracting for Aristotle to administer their programs for individual notice and consent, common consent, and/or parental access and review.

Definitions

Child means an individual under the age of 13.

Children means individuals under the age of 13.

Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:

(a) Requesting, prompting, or encouraging a child to submit personal information online;

(b) Enabling a child to make personal information publicly available in identifiable form. An operator shall not be considered to have collected personal information under this paragraph if it takes reasonable measures to delete all or virtually all personal information from a child's postings before they are made public and also to delete such information from its records; or

(c) Passive tracking of a child online.

Commission means the Federal Trade Commission.

Delete means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.

Disclose or disclosure means, with respect to personal information:

(a) The release of personal information 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

(b) Making personal information 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.

Internet means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

Online contact information means an email 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.

Operator means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of 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 involving commerce:

(a) Among the several States or with 1 or more foreign nations;
(b) In any territory of the United States or in the District of Columbia, or between any such territory and
(1) Another such territory, or
(2) Any State or foreign nation; or
(c) Between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

Personal information is *collected or maintained on behalf of* an operator when: (a) it is collected or maintained by an agent or service provider of the operator; or (b) the operator benefits by allowing another person to collect personal information directly from users of such website or online service.

Parent includes a legal guardian.

Person means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

Personal information means individually identifiable information about an individual collected online, including:

(a) A first and last name;
(b) A home or other physical address including street name and name of a city or town;
(c) Online contact information as defined in this section;
(d) A screen or user name where it functions in the same manner as online contact information, as defined in this section;
(e) A telephone number;
(f) A Social Security number;
(g) 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;
(h) A photograph, video, or audio file where such file contains a child's image or voice;
(i) Geolocation information sufficient to identify street name and name of a city or town; or
(j) 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.

Release of personal information means the sharing, selling, renting, or transfer of personal information to any third party.

Support for the internal operations of the website or online service means those activities necessary to:

(a) maintain or analyze the functioning of the website or online service;
(b) perform network communications;
(c) authenticate users of, or personalize the content on, the website or online service;
(d) serve contextual advertising on the website or online service or cap the frequency of advertising;
(e) protect the security or integrity of the user, website, or online service;
(f) ensure legal or regulatory compliance; or
(g) fulfill a request of a child as permitted by §§ 312.5(c)(3) and (4) of the COPPA Rule, in accordance with Requirement 3 D of the Program Requirements;

so long as the information collected for the activities listed in paragraphs (a)-(g) is not used or disclosed to contact a specific individual, including through behavioral advertising, to amass a profile on a specific individual, or for any other purpose.

Third party means any person who is not:

(a) An operator with respect to the collection or maintenance of personal information on the website or online service; or
(b) A person who provides support for the internal operations of the website or online service and who does not use or disclose information protected under this part for any other purpose.

Obtaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

(a) Receives notice of the operator's personal information collection, use, and disclosure practices; and
(b) Authorizes any collection, use, and/or disclosure of the personal information.

Website or online service directed to children means a commercial website or online service, or portion thereof, that is targeted to children:

(a) In determining whether a website or online service, or a portion thereof, is directed to children, the Commission will consider its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, as well as whether advertising promoting or appearing on the website or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience.

(b) A website or online service shall be deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another website or online service directed to children.

(c) A website or online service that is directed to children under the criteria set forth in (a) above, but that does not target children as its primary audience, shall not be deemed directed to children if it: (i) does not collect personal information from any visitor prior to collecting age information; and (ii) prevents the collection, use, or disclosure of personal information from visitors who identify themselves as under age 13 without first complying with the notice and parental consent provisions of this part.

(d) A website or online service shall not be deemed directed to children solely because it refers or links to a commercial website or online service directed to children by using information location tools, including a directory, index, reference, pointer, or hypertext link.

Requirement 1: <u>Notice/Disclosure of Information</u>

Members who are operators of any website or online service directed to children, or who have actual knowledge that their website or online service is collecting or maintaining personal information from children, must post a prominent link that is clearly labeled "Privacy Policy" or such similar notice that links the children to a description of the Member's information collection, use and disclosure practices, may display the Children's Mark and must abide by these requirements as set forth herein. For any section of Member's Site that is directed at children, Member may display Aristotle's Children's Mark on such section(s) of the Site, and on no other sections, and must abide by these Program Requirements.

Members must notify the Children's Privacy Compliance Program if their online information practices change or when there are planned changes to the Member's privacy policy. The Children's Privacy Compliance Program must review and approve these changes prior to any implementations of changes.

The Privacy Policy shall be displayed as follows:

i. The Site must provide a link to the Privacy Policy in a clear and prominent place and manner on: a) Member's home or landing screen or page; and b) in close proximity to any area where children directly provide, or are asked to provide, Personal Information. If the Site has a separate children's area, Member must also provide a link to the Privacy Policy in a clear and prominent place and manner on the home or landing screen or page of that area. The link at each such location must clearly indicate that the Privacy Policy includes information about the Site's information practices with regard to children.

ii. The Privacy Policy must reside on Member's server (or that of a third party with whom Member has contracted for use of a server for the Site) unless otherwise agreed to in writing or email by Aristotle and Member. Member must provide Aristotle with the URL(s) of any Privacy Policy and must provide Aristotle written or electronic notice two (2) business days prior to changing the URL(s) of any Privacy Policy.

iii. Member may label the link to the Privacy Policy with the Aristotle mark listed in Section 2 of the Membership Agreement (Children's Mark) or a hypertext link or button with the phrase "Privacy Policy." The Children's Mark or the hypertext link must link directly to the Site's Privacy Policy.

iv. The Aristotle Mark(s) listed in Section 2 of the Agreement **(**Children's Mark), hypertext link or button must link directly to the Site's Privacy Policy.

v. The Verify Mark may be located at the top of the Privacy Policy, in either margin. The Verify Mark must link to Member's Verification Page (in the form of Appendix 1 hereto) located on Aristotle's secure server at the Aristotle website. The verification page will confirm the Site's participation in the Aristotle Program.

Aristotle will assist in drafting or modifying privacy policies. Privacy Policies must be clear and understandable, and should not contain unrelated, promotional, contradictory, or confusing material. The privacy policies must be reconciled with Terms of Use, Terms of Service or End User License Agreement, so that activities on a site and all posted policies are consistent. Privacy Policies must describe the following information:

A. Notice of last update: Members must include a notice at the top of the privacy policy clearly stating when it was last updated.

B. Member Contact Information: Members must include their complete contact information. Such information must include the name, physical address, telephone number, and email address of all operators collecting or maintaining personal information from children through the website or online service. Members may list the name, address, phone number, and e-mail address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the website or online service are also listed in the notice;

C. Types of Personal Information Collected: Members must describe what information all Operators on the Member's site collect from children, including whether the website or online service enables a child to make personal information publicly available, and whether the personal information is collected directly or passively.

D. Use of Personal Information: Members must describe how personal information is used.

E. Disclosure of Personal Information: Members must state whether personal information is disclosed to third parties. If the Member does disclose personal information, the Member must: (1) describe the types of business in which such third parties are engaged and the general purposes for which the information is used; (2) state that the third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the Member; and (3) state that the parent has the option to consent to the collection and use of their child's personal information without consenting to the disclosure of that information to third parties.

F. Control Over Personal Information: Members must state in their privacy policies the choices available to the parent and the child regarding how the child's personal information is collected and used.

G. Access to Information, Deletion, and Refusal to Permit Further Collection or Use: Members must state that parents can review the child's personal information, have such information deleted, and refuse to permit further collection or use of the child's information. Members must also indicate the procedures that the parent must follow for doing so.

H. Data Security and Protection: Members must state a) that they have established and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children; and b) that they take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.

I. Questions/Complaints: Members must state in their privacy policies where the parent or child can address any questions or complaints that they may have about the website information practices. Members must include the information on how to submit complaints about the Member's websites directly to the Children's Privacy Compliance Program.

Requirement 2: <u>Direct Notice to Parents</u>

A Member must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives direct notice of the Member's practices with regard to the collection, use, or disclosure of personal information from children, including notice of any material change in the collection, use, or disclosure practices to which the parent has previously consented. The notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials.

Direct Notices to Parents must therefore contain the following information:

A. *Notice to Obtain Parent's Affirmative Consent to the Collection, Use, or Disclosure of a Child's Personal Information*.

This direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child, and, if such is the case, the name of the child or the parent, in order to obtain the parent's consent;
(ii) That the parent's consent is required for the collection, use, or disclosure of such information, and that the operator will not collect, use, or disclose any personal information from the child if the parent does not provide such consent;
(iii) The additional items of personal information the operator intends to collect from the child, or the potential opportunities for the disclosure of personal information, should the parent provide consent;
(iv) A hyperlink to the Member's Privacy Policy;
(v) The means by which the parent can provide verifiable consent to the collection, use, and disclosure of the information; and
(vi) That if the parent does not provide consent within a reasonable time from the date the direct notice was sent, the operator will delete the parent's online contact information from its records.

B. *Voluntary Notice to Parent of a Child's Online Activities Not Involving the Collection, Use or Disclosure of Personal Information.*

Where an operator chooses to notify a parent of a child's participation in a website or online service, and where such site or service does not collect any personal information other than the parent's online contact information, the direct notice shall set forth:

(i) That the operator has collected the parent's online contact information from the child in order to provide notice to, and subsequently update the parent about, a child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information;
(ii) That the parent's online contact information will not be used or disclosed for any other purpose;
(iii) That the parent may refuse to permit the child's participation in the website or online service and may require the deletion of the parent's online contact information, and how the parent can do so; and
(iv) A hyperlink to the Member's Privacy Policy.

C. *Notice to a Parent of Operator's Intent to Communicate with the Child Multiple Times.*

This direct notice shall set forth:

(i) That the operator has collected the child's online contact information from the child in order to provide multiple online communications to the child;
(ii) That the operator 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 from the operator;
(iii) That the online contact information collected from the child will not be used for any other purpose, disclosed, or combined with any other information collected from the child;
(iv) That 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) That if the parent fails to respond to this direct notice, the operator may use the online contact information collected from the child for the purpose stated in the direct notice; and
(vi) A hyperlink to the Member's Privacy Policy.

D. *Notice to a Parent In Order to Protect a Child's Safety*.

This direct notice shall set forth:

(i) That the operator has collected the name and the online contact information of the child and the parent in order to protect the safety of a child;
(ii) That the information will not be used or disclosed for any purpose unrelated to the child's safety;
(iii) That the parent may refuse to permit the use, and require the deletion, of the information collected, and how the parent can do so;
(iv) That if the parent fails to respond to this direct notice, the operator may use the information for the purpose stated in the direct notice; and
(v) A hyperlink to the Member's Privacy Policy.

Requirement 3: <u>Prior Verifiable Parental Consent</u>

A. <u>Generally</u>: Except as provided in Sections 3(C) and 3(D), Members must obtain verifiable parental consent before any collection, use, display, or disclosure of personal information from children, and will make best efforts to prevent a child from making such information public without such consent. This includes, but is not limited to, public posting through the Internet, a home page of a website, a pen pal service, an electronic mail service, a message board, or a chat room.

Members must also obtain such consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented. Changes are material under this subsection if they relate to Member's practices regarding collection, use, or disclosure of Personal Information; notice and disclosure regarding those practices; user choice and consent regarding how Personal Information is used and shared; or measures for data security, integrity, or access. If Member materially changes its privacy practices, Member must follow Requirements 2 and 3 and provide notice and obtain verifiable parental consent before collecting, using, or disclosing Personal Information from children for the new practices. Members must notify the Children's Privacy Compliance Program when making material changes to their Privacy Policy, and may be subject to a revision fee.

Members must give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties.

Member shall notify Aristotle prior to (i) any Assignment or Transfer which involves sharing Personal Information between the parties; (ii) change in name of Member or (iii) change of domain name for the Site. An Assignment or Transfer of Personal Information shall be treated as a transfer to a third party of Personal Information collected by Member, and the Member must follow Requirement 2 with regard to providing parental notice and choice. Alternatively, with the prior written consent of Aristotle, which consent shall not be unreasonably withheld or delayed, Member may post prominent notices on the Site about the Assignment or Transfer provided such notices are posted for at least thirty (30) consecutive business days prior to completion of the Assignment or Transfer, where notice and verifiable parental consent are not required. If Member ceases to exist or is not the controlling entity as a result of a merger, acquisition or other organizational change, the successor of the company must meet Aristotle criteria in order to carry any Aristotle Mark(s).

B. <u>Method for Obtaining Verifiable Parental Consent</u>: To comply with Requirement 3 (Verifiable Parental Consent), Members must obtain prior verifiable parental consent. Any method to obtain prior verifiable parental consent must be reasonably calculated, in light of the available technology, to ensure that the person providing consent is the child's parent. Methods to obtain prior verifiable parental consent include: i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan; (ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder; (iii) Having a parent call a toll-free telephone number staffed by trained personnel; (iv) Having a parent connect to trained personnel via video-conference; (v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information; or (vi) using the Integrity System, a suite of online and offline methods by which an individual can authenticate his or her identity and therefore activate an account in order to provide member sites with notice and verifiable consent. The Integrity System provides a total of thirteen (13) methods of verification. The eleven online mechanisms include: (i) the verification of the last four digits of the individual's social security number; (ii) verification of the individual's driver license number; (iii) in connection with a monetary transaction, the use of a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder; (iv) email

with an electronically signed parental consent form, and verification of an attached photo, scan or copy of a form of government-issued identification (e.g., voter registration card, driver's license, other official license), where the parent's identification is deleted by the operator from its records promptly after such verification is complete; (v) email with an attached photo, scan or electronic copy (e.g., pdf format) of a physically signed parental consent form; (vi) the electronic submission through a secure website (upload) and verification of an attached photo, scan or copy of form of government-issued identification, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; (vii) the electronic submission through a secure website (upload) and verification of an attached photo, scan or copy of a physically signed parental consent form; (viii) electronic transmission and verification of a photo, scan or copy of a form of government-issued identification through Multimedia Messaging Service ("MMS"), where the parent's identification is deleted by the operator from its records promptly after such verification is complete; (ix) electronic transmission and verification of a photo, scan or copy of a physically signed parental consent form through Multimedia Messaging Service ("MMS"); (x) submission of the full name, birth date, and location of the parent, and government-issued identification number (SSN4, Driver's License Number, Passport Number, State ID Number) verified through the use of a commercially available database or aggregate of databases, consisting primarily of data from government sources, that are regularly used by government and businesses for the purpose of age and identity verification and authentication, where the parent's identification is deleted by the operator from its records promptly after such verification is complete; and (xi) face-to-face real-time verification through online telephony or videoconferencing technology. The two offline methods include (i) printing out a parental consent form, signing it, and mailing or faxing the form to the Children's Privacy Compliance Program, and (ii) providing consent over the telephone using a toll-free number staffed by trained operators.

Integrity may approve additional methods of obtaining Verifiable Parental Consent for Members that are reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.

The Integrity system may collect personal information as part of the Prior Verifiable Parental Consent process. Secure handling and storage of such information is of the utmost and highest concern. All Personal Information submitted to Integrity, and the transaction ID number assigned to each verification request shall be stored on separate servers and separate databases independent of all other corporate data, stored in a secure encrypted form immediately after submission, and the parent's identification shall be deleted as indicated above.

All transmissions of data are in a secure communication protocol. We maintain physical, electronic and procedural safeguards to protect Personal Information that meet or exceed industry standards, and following completion of the verification transaction, the stored data shall be used only for auditing purposes pertaining to the accuracy of the verification and for no other use.

C. Where Member Does Not Disclose Children's Personal Information: A member operator that does not "disclose" children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email.

D. Exceptions to Verifiable Parental Consent: The exceptions to prior verifiable parental consent are as follows:

- *Required Parental Consent* - Where the sole purpose of collecting the name or online contact information of the parent or child is to provide notice and obtain parental consent to the Collection, Use, or Disclosure of a Child's Personal Information under Requirement 2(A). If the Member has not obtained parental consent after a reasonable time from the date of the information collection, the Member must delete such information from its records.

- *Voluntary Notice Under Requirement 2(B)* - Where the purpose of collecting a parent's online contact information is to provide voluntary notice to, and subsequently update the parent about, the child's participation in a website or online service that does not otherwise collect, use, or disclose children's personal information. In such cases, the parent's online contact information may not be used or disclosed for any other purpose. In such cases, the Member must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in Requirement 2(B).

- *One-Time Request* –Where the sole purpose of collecting online contact information from a child is to respond directly on a one-time basis to a specific request from the child, and where such information is not used to re-contact

the child or for any other purpose, is not disclosed, and is deleted by the operator from its records promptly after responding to the child's request.

- *Multiple Requests* – Where the purpose of collecting a child's and a parent's online contact information is to respond directly more than once to the child's specific request, and where such information is not used for any other purpose, disclosed, or combined with any other information collected from the child. In such cases, the Member must make reasonable efforts, taking into consideration available technology, to ensure that the parent receives notice as described in Requirement 2(C). A Member 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.

- *Child Safety* - Where the purpose of collecting a child's and a parent's name and online contact information, is to protect the safety of a child, and where such information is not used or disclosed for any purpose unrelated to the child's safety. In such cases, the Member must make reasonable efforts, taking into consideration available technology, to provide a parent with notice as described in Requirement 2(D).

- *Additional Safety Concerns* - Members may collect a child's first name or online contact information to protect the security or integrity of the website or online service, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or for investigations on matters related to public safety, so long as the information is not used for any other purpose. Direct notice is not required under this exception.

- *Persistent Identifier Used Solely in Support of Internal Operations* – Where a persistent identifier and no other personal information is collected and such identifier is used for the sole purpose of providing support for the internal operations of the website or online service. In such case, there also shall be no obligation to provide notice.

- *Certain Conditions Where Member Covered Under Paragraph (b) of the Definition of Website or Online Service Directed to Children Collects a Persistent Identifier* - Where a Member covered under paragraph (b) of the definition of *website or online service directed to children* collects a persistent identifier and no other personal information from a user who affirmatively interacts with the Member and whose previous registration with that Member indicates that such user is not a child. In such case, there also shall be no obligation to provide notice under § 312.4.

Requirement 4: <u>Access and Review</u>

Members must provide parents with the ability to access and review their child's personal information.

(a) Upon request of a parent whose child has provided personal information to a Member, the Member is required to provide to that parent the following:

(1) A description of the specific types or categories of personal information collected from children by the Member, such as name, address, telephone number, e-mail address, hobbies, and extracurricular activities;

(2) The opportunity at any time to refuse to permit the Member's further use or future online collection of personal information from that child, and to direct the Member to delete the child's personal information; and

(3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the Member to carry out this provision must:

(i) Ensure that the requestor is a parent of that child, taking into account available technology; and

(ii) Not be unduly burdensome to the parent.

(b) Neither a Member nor the Member's agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section.

(c) Subject to the limitations set forth in Requirement 5, a Member may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the Member's further use or collection of personal information from his or her child or has directed the Member to delete the child's personal information.

Requirement 5: Restrictions on Information Collection

A child-directed site may not use an age gate.

The age information on the registration form of a site not directed to children or where children are not the primary audience must be asked in a neutral manner that does not invite falsification. Members must employ temporary or permanent cookies to prevent children from back-buttoning to change their age in order to circumvent the parental consent requirement or obtain access to the site**.**

Members are prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

Requirement 6: Confidentiality, Security and Integrity of Information

A Member shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected. The Member must delete such information using reasonable measures to protect against unauthorized access to, or use of, the information in connection with its deletion.

The Member must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The Member must also take reasonable steps to release children's personal information only to service providers and third parties who are capable of maintaining the confidentiality, security and integrity of such information, and who provide assurances that they will maintain the information in such a manner.
If Member collects, uses, discloses or distributes sensitive information, such as credit card numbers or social security numbers, it shall utilize appropriate commercially reasonable practices, such as encryption, to protect information transmitted over the Internet.

Requirement 7: Compliance/Enforcement

A. Program Representative: Members must appoint a program representative for the website(s). The program representative shall be the individual responsible for overseeing the website compliance with the Children's Privacy Compliance Program. The program representative shall be given the authority to investigate all inquiries concerning the website's privacy policy and information practices and in a timely manner. Aristotle agrees to name an account manager for Member within fifteen (15) business days of the Effective Date by providing written or electronic notice to Member. All notices between Aristotle and Member shall be directed to the designated Program Representative and designated Aristotle account manager, which either party may change upon written or electronic notice to the other.

B. Initial and Annual Self-Evaluation: Members must conduct an evaluation of their website information collection, use, and disclosure practices. Each Member will be required to complete and attest to the accuracy of the statements they make on a Self-Evaluation form (Appendix 2 to these Program Requirements] about their information practices. Once Aristotle receives the Self-Evaluation form, an Aristotle representative will independently review the website's posted privacy policy, information practices, and the Self-Evaluation form for compliance with the Program Requirements. Once the Member website is determined to be in full compliance with the Program Requirements, it will then be listed as a Member participating in the Children's Privacy Compliance Program. Members are required to complete a Self-Evaluation form on an annual basis to ensure that their websites' information practices are consistent with their posted privacy policies and the Program Requirements.

C. Compliance Monitoring: Members must submit to monitoring of their website information practices. The purpose of monitoring reviews is to ensure that a Member's privacy policy is consistent with its website information practices. Monitoring reviews also allow the Children's Privacy Compliance Program or an independent third party designated by the Children's Privacy Compliance Program to verify that the Member's website complies with the Program Requirements at all times. The compliance monitoring may be conducted on a quarterly basis, but in no event less than annually. In addition to such monitoring, Members must also agree to submit to periodic, unannounced reviews of their websites. These unannounced reviews will be used to further verify that the Member remains in full compliance with the Program Requirements.

If the Children's Privacy Compliance Program determines that a violation of the requirements has occurred the Member is informed of such violation and the corrective actions that must be taken to bring the Member's website into compliance. Failure to take the corrective actions can result in a number of consequences including removal from the Children's Privacy Compliance Program and referral to the appropriate governmental agency.

D. Consumer Complaints/Monitoring: Members must provide the parent and the child with reasonable and effective means to submit complaints that they may have about the Member's information practices. The Children's Privacy Compliance Program also offers the parent and the child the opportunity to submit complaints about any Member directly to Aristotle's Dispute Resolution Process. A Children's Privacy Compliance Program representative responds to all complaints immediately. Members must agree to work with Aristotle representatives in their efforts to resolve all complaints that are submitted to the Children's Privacy Compliance Program Dispute Resolution Process. If Member has materially breached this Agreement, Member agrees to reimburse Aristotle for the reasonable cost of any such review and promptly rectify the practice to the Children's Privacy Compliance Program's reasonable satisfaction. Members must maintain records for a period of three (3) years of all complaints, concerns, or inquiries received about its website and any responses to the consumer addressing such complaint or concern.

E. Membership Agreement: Members must execute the Children's Privacy Compliance Program membership agreement. As part of this agreement, Members agree to comply with the Program Requirements at all times. In the event that a Member fails to meet any of its obligations under the membership agreement, such actions would constitute a material breach of the agreement and its membership in the Children's Privacy Compliance Program would be terminated.

F. Investigations/Referral to Governmental Agencies: If the Children's Privacy Compliance Program's determines, after a thorough investigation into the Member information practices that a Member has violated its posted privacy policy or any of the requirements described above, the Children's Privacy Compliance Program's may refer such Member to the Federal Trade Commission for possible unfair and deceptive trade practices.

G. Reporting Requirements: Members are provided detailed reports on results of audits, disciplinary actions and consumer complaints. Aristotle maintains a record of the results of audits, disciplinary actions and consumer complaints for a period of at least three (3) years and is made available to the member company.

Integrity Children's Privacy Compliance Program

APPENDIX 1 TO INTEGRITY CHILDREN'S PRIVACY COMPLIANCE PROGRAM REQUIREMENTS:

Verification Page Text

Version No: 2.4
Last Updated: June 11, 2013

The following verification page will be used for Member's sites.

(Name of the Company) is a Member of the Aristotle Integrity's Children's Privacy Compliance Program. This Privacy Policy discloses the privacy practices for (URL of the Site).

Aristotle is a private, for-profit organization committed to building users' trust and confidence in the Internet by promoting the use of fair information practices. Because this site wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed for compliance by Aristotle. This website complies with the Aristotle Integrity Children's Privacy Compliance Program, which has been approved by the Federal Trade Commission as an authorized safe harbor under the Children's Online Privacy Protection Rule. When you and your child visit a website displaying the Aristotle Integrity Children's Privacy Compliance "Click to Verify" trust mark, you can expect to be notified of:

a. What Personal Information the website seeks to collect from your child;

b. The organization(s) collecting the information;

c. How the information is used;

d. With whom the information may be shared;

e. What choices are available to you regarding collection, use and distribution of the information collected from your child;

f. The kind of security procedures that are in place to protect the loss, misuse or alteration of information under (Name of the Company) control;

g. How you can review and delete any information collected from your child;

h. Where relevant, How you can opt not to share Personal Information collected from your child with third parties, if you so choose.

If you have questions or concerns regarding this statement, you should first contact (insert name of individual, department or group responsible for inquiries) by (insert contact information; email, phone, postal mail, etc.) If you do not receive acknowledgment of your inquiry or your inquiry has not been satisfactorily addressed, you should then contact the Aristotle Dispute Resolution Program at http://privacy.integrity.aristotle.com. Aristotle will then serve as a liaison with the website to resolve your concerns.

Aristotle Membership Agreement Version ___[**Member must fill in version of**

Aristotle Membership Agreement under which it is operating]

Integrity Children's Privacy Compliance Program

Appendix 2 to Integrity Children's Privacy Compliance Program Requirements

Self-Evaluation Review Report

(Redacted From Public Record Version)

Version No: 2.4
Last Updated: June 11, 2013
Version Notes: Updates Program to Comply with Children's Online Privacy Protection Rule ("Final Rule") (16 C.F.R. Part 312)

Integrity Children's Privacy Compliance Program

Exhibit B to Integrity Children's Privacy Compliance Program Membership Agreement

Sample Marks

Version No: 2.4
Last Updated: June 11, 2013

Graphical user image provided by Aristotle that shall activate a link to access directly an Aristotle server for authentication purposes.

Sample Verify Mark and Membership Certification/Privacy Statement Mark

Integrity Children's Privacy Compliance Program

Exhibit 2 to Request for Safe Harbor Approval by the Federal Trade Commission for Aristotle International, Inc.'s Integrity Safe Harbor Compliance Program Under Section 312.11 of the Children's Online Privacy Protection Rule.

Monitoring Review Report

(Redacted From Public Record Version)

Version No: 2.4
Last Updated: June 11, 2013
Version Notes: Updates Program to Comply with Children's Online Privacy Protection Rule ("Final Rule") (16 C.F.R. Part 312)