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
3635 Ruffin Rd., Floor 3
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
622 N 900 E., Suite 2
Spanish Fork, UT 84660
p (801) 798-0673
f (801) 798-6794

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

February 22, 2012

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

RE: 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.

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 312.10 implementing the Children's Online Privacy Protection Act (15 U. S. C. sec. 6501 et. seq.).

[If necessary: In addition to this original, Aristotle submits five (5) copies of this revised application for safe harbor approval, along with a compact disc containing the revised application in Microsoft Word format.]

Aristotle's Integrity Children's Privacy Compliance Program is modeled after previous safe harbor programs approved by the FTC, with several improvements addressing new technologies and providing additional privacy enhancement. Principal among these improvements and enhancements are the use of electronic real-time face-to-face verification of a parent via Skype or similar videoconferencing technologies, scanning and emailing or uploading of consent forms and government-issued identification, and the ability to check government-issued identification against our own extensive databases without the need to send data out to third parties for verification. We believe that this program will benefit and protect more children and legitimate websites catering to them, particularly those social networks wishing to comply with COPPA.

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

Part I includes (A) a brief description of Aristotle and its Integrity Children's Privacy Compliance Program and (B) the full text of the Integrity Children's Privacy Compliance Program Requirements ("Program Requirements") for which approval is sought by the Federal Trade Commission ("Commission").

Part II includes a comparison of each provision of Section 312.3 through Section 312.8 with the corresponding provisions of the Program Requirements; and

Part III includes a statement explaining (A) how the Program Requirements and applicable assessment mechanisms meet the requirements of the Final Rule, and (B) how the assessment mechanisms and compliance incentives required under Section 312.10(b) (2) and (3) provide effective enforcement of the requirements of the Final Rule.

Attached to Aristotle's application are the following documents (those documents marked with an asterisk are proprietary and are to be redacted from the public record version):

- Exhibit 1: Integrity Children's Privacy Compliance Program Membership Agreement*
    - Exhibit A to Membership Agreement: Program Requirements
        - Appendix 1 to Program Requirements: Verification Page
        - Appendix 2 to Program Requirements: Self-Evaluation Form*
    - Exhibit B to Membership Agreement: Sample Marks
- Exhibit 2: Monitoring Review Report Form

Aristotle wishes to thank the Commission in advance for its consideration. We look forward to working with the Commission during the review and approval process.

Respectfully submitted,

J. Blair Richardson
General Counsel and Chief Privacy Officer
Aristotle International, Inc.
Integrity Children's Privacy Compliance Program

PART I. BACKGROUND INFORMATION ON ARISTOTLE AND A COPY OF THE FULL TEXT OF THE CHILDREN'S PRIVACY COMPLIANCE PROGRAM REQUIREMENTS

I (A) ARISTOTLE AND THE CHILDREN'S PRIVACY COMPLIANCE PROGRAM

Introduction

The Integrity Children's Privacy Compliance Program is an independent compliance and enforcement program that assists companies in protecting information obtained from children online. Our program helps companies safeguard the rights of children by providing guidelines that companies can follow to ensure that the information they obtain from children is done in an open, secure, and reliable manner. From our Program Requirements for the collection, use and disclosure of personal information from children, to our Integrity System, our proprietary verifiable parental consent mechanism, we offer companies an integrated privacy program that is dedicated to the protection of personal information from children online.

Background

Aristotle's Integrity division was established in 1999 in response to the increased need for effective and meaningful technological solutions to verify age and identity online, including the need to enable companies to create rewarding relationships with children online while meeting the expectations and concerns of parents and governmental regulators. Integrity is a global leader in online age and identity verification, and has performed millions of verifications across various industries.

Since passage of the Children's Online Privacy Protection Act ("COPPA") there has been a need for trusted, neutral privacy programs that focus on the collection of information from children in an efficient and compliant way.

As a leading provider of age and identity verification, and building on its knowledge of the Children's Online Privacy Protection Act ("COPPA"), Aristotle seeks approval for its Integrity Children's Privacy Compliance Program.

The Integrity Children's Privacy Compliance Program is a truly integrated privacy program that provides parents and children with the ability to manage their personal information that a website obtains from them, and companies with the confidence that the information they obtained from children is compliant with COPPA.

Program Requirements Overview

Member companies must agree to abide by the Program Requirements. The Program Requirements are a set of guidelines that regulate the way member companies collect, use and disclose personal information from children 12 years old and under. By following the Program Requirements, visitors to websites operated by a member company are assured that:

A privacy policy will be posted on the homepage of a member company's website and a link to such privacy policy will be provided at each point within the website where personal information is collected;

Notice will be provided to the child's parent about the website's information practices and prior verifiable consent will be obtained before collecting personal information from children;

The child's parent will be given the choice to consent to the collection and use of their child's personal information for internal use by the website, and the parent will be given the opportunity to elect not to have their child's personal information disclosed to third parties;

The parent will be provided with access to their child's personal information, and given the ability to review and/or delete the information and opt-out of the future collection or use of the information;

The age information on the registration form 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;

The child's participation in a game, the offering of a prize, or another activity will not be conditioned on the child's disclosure of more personal information than is reasonably necessary for the activity; and

Member companies will maintain the confidentiality, security, and integrity of the personal information they collect from children.

Integrity Membership Seal of Approval and Click-to-Verify Mark

Member companies that satisfy the Program Requirements must display the Integrity Membership Seal of Approval. For parents and children, the Membership Seal of Approval offers them assurance that the website has a posted privacy policy, that the privacy policy describes how the information is collected and used, and that website submits to ongoing monitoring and enforcement.

Visitors to websites that are members in the Children's Privacy Compliance Program can verify such membership by using the "click to verify" mark ("Verify Mark"). Each Verify Mark is linked to a verification page on a secure Aristotle server. The verification page allows parents to verify that the website is authorized to display the Integrity Membership Seal of Approval and the Verify Mark, and is in full compliance with the Program Requirements.

Compliance Advancement Team

As part of the Program Requirements, member companies must post a privacy policy that is clear, understandable and contains no unrelated contradictory or confusing material. To assist member companies with implementing a meaningful privacy policy that properly conveys to the parent and child the necessary information about the website information practices, Aristotle's Integrity offers member companies guidance on how to modify their existing privacy policy, or help with drafting their first privacy policy, to make sure that all member companies comply with the Program Requirements.

Compliance Monitoring

Compliance monitoring is a central part of the entire Children's Privacy Compliance Program and includes the following components: initial and annual self-evaluation of a member company's website; quarterly and periodic, unannounced monitoring reviews of the member company website; and community monitoring reviews.

First, all member companies must conduct an initial evaluation of their website's information collection, use, and disclosure practices. Each member company is required to complete and attest to the accuracy of the statements it makes on a self-evaluation form about its information practices. A representative of the Children's Privacy Compliance Program will independently review the website's privacy policy and practices with the self-evaluation form to ensure that they are consistent with each other, the Program Requirements, and COPPA. Before becoming a participating member in the Children's Privacy Compliance Program, the company seeking membership must make all required modifications to its website that Aristotle deems necessary to comply with the Program Requirements and COPPA. Member companies will be required to complete the same self-evaluation form on an annual basis to ensure that their website information practices continually comply with the Program Requirements and COPPA, and are consistent with their posted privacy policies.

Second, all member companies must submit to quarterly monitoring of their website's information practices. The purpose of monitoring reviews is to ensure that a member company's website and its privacy policy are constantly in full compliance with the Program Requirements and COPPA. Specifically, monitoring reviews are conducted by trained privacy monitors that systematically move about a member company website ensuring that: (i) there is a prominent link to the website's privacy policy on the homepage and any web page where information is collected by the website; (ii) the member company obtains prior verifiable parental consent from all children twelve years old and under before collecting their personal information; and (iii) there is compliance with the Program Requirements.

In addition to quarterly monitoring, a member company must also agree to submit to periodic, unannounced reviews of its website. These unannounced reviews will be used to further verify that the member company's website is complying with the Program Requirements and COPPA at all times. The Children's Privacy Compliance Program will also periodically "seed" the personal information it maintains on behalf of a member company to confirm that the member company is not using the

information for any other purposes than the stated purpose in its privacy policy. Reviews are memorialized in written reports provided to the member and maintained by the Children's Privacy Compliance Program for a period of at least three (3) years.

Third, all member companies must provide the parent and child with a reasonable and effective means to submit complaints that they may have about the member company information practices. The Children's Privacy Compliance Program also offers the parent and child the opportunity to submit complaints about any member company website directly to the Children's Privacy Compliance Program. A representative of the Children's Privacy Compliance Program handles all complaints immediately. The Children's Privacy Compliance Program maintains a record for three (3) years of all complaints received by the Children's Privacy Compliance Program, any investigation conducted by Aristotle into the alleged violation of the Program Requirements, and the outcome of such investigation.

Dispute Resolution

Member companies must provide the parent and the child with a means to submit questions or complaints that they may have about a member company's information practices. If the parent or child is not satisfied with the response they receive from the member company, the Children's Privacy Compliance Dispute Resolution Program offers parents assistance with resolving those complaints. Such assistance may include contacting the member company directly to investigate the complaint and finding a resolution of the parent's or child's concern or requiring a representative of the member company to participate in the Children's Privacy Compliance Program's alternative dispute resolution services. In both cases, a trained member of the Children's Privacy Compliance Program staff administers the process.

I (B). TEXT OF THE INTEGRITY CHILDREN'S PRIVACY COMPLIANCE PROGRAM REQUIREMENTS

INTEGRITY CHILDREN'S PRIVACY COMPLIANCE PROGRAM REQUIREMENTS

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.

Definitions

"Personal Information" means individually identifiable information about any individual collected online from a child under 13, 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) an email address or other online contact information, including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security number; (f) a persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or (g) information concerning the child or the parents of that child that the operator collects online from the child and combines with any individually identifiable information described in this definition.

Requirement 1: Notice/Disclosure of Information

Members with online activities that are directed at children under the age of 13, or that have actual knowledge that they are collecting or maintaining personal information from children under the age of 13, 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, must display the Children's Mark and must abide by this Exhibit A, Children's Program Requirements, as set forth herein. If a section of Member's Site is directed at children under 13, Member must display Aristotle's Children's Mark on that section of the Site and must abide by this Exhibit A.

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 located 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 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 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. If using a hypertext link, the text must have a 10-point minimum font size or be consistent with the size of the other menu items, whichever is larger. 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 must 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. See also http://privacy.integrity.aristotle.com/downloads/coppa-how-comply.pdf for guidance on privacy policy requirements. 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. In cases where more than one company is responsible for a website, the Member may choose to respond to all inquiries from parents concerning the Member privacy policies, provided that the names, physical addresses, telephone numbers, and email of all persons or companies collecting personal information through the website are listed in the privacy policy.

C. Types of Personal Information Collected: Members must describe the types of personal information collected 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) whether the third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the Member; and (3) 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; and (4) identify and provide information (name, physical address, telephone number, and email address) concerning any third party that is collecting personal information through the member website or with whom the member is sharing such information.

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. Restrictions on Information Collection: Members must state that they 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.

H. Access to Information: 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 to access their child's personal information.

I. Data Security and Protection: Members must state specific information disclosing the manner in which that Member intends to protect personal information (e.g. use of SSL, firewalls, other encryption methods, etc.).

J. 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

Members must make reasonable efforts to ensure that a parent of a child receives notice of the Member's information collection, use, and disclosure practices with regard to children, including notice of any material change in the collection, use, or disclosure practices to which the parent had previously consented. Mechanisms to provide notice include, but are not limited to, sending the notice to the parent's email address or sending the notice by postal mail.

Direct Notices to Parents must contain the following information:

A. Privacy Policy Information: Members must include all of the information that is necessitated as part of Requirement 1 above.

B. Purpose is to Collect Information: Members must state that they wish to collect personal information from the child.

C. Parental Consent Required: Members must state that the parent's consent is required for the collection, use, or disclosure of the child's personal information. Members must also describe the method by which a parent may give such consent.

Except for certain circumstances described below under Requirement 3(C), Members must meet the requirements described above and obtain prior verifiable parental consent before they are allowed to collect personal information from children.

Requirement 3: Prior Verifiable Parental Consent

A. Generally: Members must obtain verifiable parental consent before any collection, use, display, or disclosure of personal information from children under 13, and will make best efforts to prevent a child from doing so 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 Section 3(B) 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 may be subject to a revision fee.

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 section 3(A) 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. 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 Member by postal mail or facsimile; (ii) requiring the parent to use a credit card in connection with a transaction; (iii) having a parent call a toll- free telephone number staffed by trained personnel; or (iv) 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 verifiable permission. 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) the use of a credit card in connection with a transaction; (iv) email with an electronically signed parental consent form, and verification of an attached copy of a government-issued identity document (e.g., voter registration card, driver's license, other official license); (v) email with an attached 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 copy of a government-issued identity document; (vii) the electronic submission through a secure website (upload) and verification of an attached copy of a physically signed parental consent form; (viii) electronic transmission and verification of a photocopy of a government-issued identity document through Multimedia Messaging Service ("MMS"); (ix) electronic transmission and verification of a photocopy 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 identity document 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; 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.

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 away from all other corporate data. All Personal Identity Document numbers ("PID numbers") submitted during this process (*e.g.*, SSN4, Driver's License Number, Passport number) shall be stored in a secure encrypted form immediately after submission, and all such PID numbers shall be deleted a reasonable time after submission. Should new rules be adopted to require immediate deletion of any information, such change will be implemented.

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 no other.

C. Exceptions to Verifiable Parental Consent: Even though verifiable parental consent is required under most situations before a Member is permitted to collect, use, or disclose a child's personal information, there are a few exceptions where a Member will

be allowed to collect a child's first name or online contact information before obtaining consent from the child's parent. The exceptions to prior verifiable parental consent are as follows:

- *Required Parental Consent* - Members may collect the first name or online contact information of a child to be used for the sole purpose of obtaining the parental consent. If a 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. Members that collect the first name or online contact information from a child under this exception must provide direct notice to the parent. The direct notice must include all privacy policy information (*See* Requirement 2 (A), above) and notify the parent that the Member has collected the child's first name and email address to respond to and obtain consent from the parent. If the Member has not obtained parental consent after a reasonable time from the date the information is collected, the Member must delete such information from its records.

- *One-Time Request* – Members may collect the online contact information of child for the sole purpose of responding directly, on a one-time basis, to a specific request from the child. Members that collect the online contact information from a child under this exception must not use the information to recontact the child after the initial response and must delete the child's personal information. Direct notice is not required under this exception.

- *Multiple Requests* – Members may collect the online contact information from a child to be used to respond directly more than once to a specific request from the child so long as the information is not used for any other purpose. Members that obtain the online contact information from a child under this exception must provide direct notice to the parent. The direct notice must: (1) include all privacy policy information (*See* Requirement 2 (A), above); (2) notify the parent that the Member has collected the child's online contact information to respond to the child's request; (3) explain the nature and intended use of the information; (4) inform the parent that they may request that the Member make no further use of the information and that such information be deleted; (5) describe the procedures by which the parent can refuse to allow further contact and information collection from the child; and, (6) explain that if the parent does not opt out, the Member may use the information for the purposes stated in the direct notice. The direct notice must be sent after the initial response and before making any additional response to the child.

- *Child Safety* - Members may collect the child's first name or online contact information to the extent reasonably necessary to protect the safety of a child participant on the website where the Member used reasonable efforts to provide notice to the parent. The information collected by Member under this exception must be used for the sole purpose of protecting the child's safety, must not be used to re-contact the child or for any other purpose than for the purpose stated in this exception and must not be disclosed by a Member on its website. The direct notice must: (1) include all privacy policy information (*See* Requirement 2(A), above); (2) notify the parent that the Member has collected the child's online contact information to protect the safety of the child participating on the website; (3) inform the parent that they may refuse to permit the use of the information and may require its deletion, and inform them how they can have the information deleted; and, (4) explain that if the parent does not opt out, the Member may use the information for the purposes stated in the direct notice.

- *Additional Safety Concerns* - Members may collect a child's first name or online contact information to protect the security or integrity of the website, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or 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.

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

Members must provide parents with the ability to access and review their child's personal information. Parental review and access must consist of: (a) a description of the specific types of personal information collected from the child; (b) the opportunity at any time to refuse to permit the Member from further using or collecting the child's personal information; and (c) the ability to direct the Member to delete the child's personal information from the Member records.

In addition to providing the ability for a parent to access and review their child's personal information, Members must take reasonable steps to ensure that the individual requesting access is the child's parent. Acceptable steps for authenticating the identity of the individual online include a username and password unique to the individual or, if access is requested over the

telephone, asking a series of questions that only a parent of the child would have knowledge of (e.g., parent's name, mailing address, email address, child's name, child's email address, etc.).

Requirement 5: Restrictions on Information Collection

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.

The age information on the registration form 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;

Requirement 6: Confidentiality, Security and Integrity of Information

Members must disclose their data retention and deletion policies/practices and only retain data that is necessary for ongoing business operations.

Members must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. 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 will be conducted on a quarterly basis. In addition to the quarterly 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.

PART II: A COMPARISON OF EACH PROVISION OF SECTION 312.3 THROUGH SECTION 312.8 WITH THE CORRESPONDING PROVISIONS OF THE CHILDREN'S PRIVACY COMPLIANCE PROGRAM REQUIREMENTS.

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 information collection, use, and disclosure practices with regard to 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): Member companies must obtain verifiable consent before any collection, use, or disclosure of personal information from children unless permitted to collect the child's name or online contact information 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 Section of the Children's Privacy Compliance Program Requirements:

Requirement 1: Notice/Disclosure of Information

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

The privacy policy link must be plainly visible on the homepage and on each web page where personal information is collected from children and in close proximity to the requests for information in each such area. For general audience websites, the privacy policy link must be plainly visible on the first page of the children's section of the website.

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. In cases where more than one company is responsible for a website, the Member may choose to respond to all inquiries from parents concerning the Member privacy policies, provided that the names, physical addresses, telephone numbers, and email of all persons or companies collecting personal information through the website are listed in the privacy policy.

C. Types of Personal Information Collected: Members must describe the types of personal information collected 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) whether the third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the Member; and (3) 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; and (4) identify and provide information (name, physical address, telephone number, and email address) concerning any third party that is collecting personally information through the member website or with whom the member is sharing such information.

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. Restrictions on Information Collection: Members must state that they 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.

H. Access to Information: 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 to access their child's personal information.

I. Data Security and Protection: Members must state specific information disclosing the manner in which that Member intends to protect personal information (e.g. use of SSL, firewalls, other encryption methods, etc.).

J. 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.

Section 312.5: *Parental consent.*

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

Requirement 3: Prior Verifiable Parental Consent

A. Generally: 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.

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 Member by postal mail or facsimile; (ii) requiring the parent to use a credit card in connection with a transaction; (iii) having a parent call a toll-free telephone number staffed by trained personnel; or (iv) using the Integrity System.

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.

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. Parental review and access must consist of: (a) a description of the specific types of personal information collected from the child; (b) the opportunity at any time to refuse to permit the Member's further using or collecting the child's personal information; and (c) the ability to direct the Member to delete the child's personal information from the Member's records.

In addition to providing the ability for a parent to access and review their child's personal information, Members must take reasonable steps to ensure that the individual requesting access is the child's parent. Acceptable steps for authenticating the identity of the individual online include a username and password unique to the individual or, if access is requested over the telephone, asking a series of questions that only a parent of the child would have knowledge of (e.g., parent's name, mailing address, email address, child's name, child's email address, etc.).

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

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.

The age information on the registration form 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;

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 disclose their data retention and deletion policies/practices and only retain data that is necessary for ongoing business operations.

Members must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. 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.

PART III: STATEMENT EXPLAINING (A) HOW THE PROGRAM REQUIREMENTS AND APPLICABLE ASSESSMENT MECHANISM MEET THE REQUIREMENTS OF THE FINAL RULE, AND (B) HOW THE ASSESSMENT MECHANISM AND COMPLIANCE INCENTIVES REQUIRED UNDER SECTION 312.10 (B) (2) AND (3) PROVIDE EFFECTIVE ENFORCEMENT OF THE REQUIREMENTS OF THE FINAL RULE.

III (A) How the Program Requirements and Applicable Assessment Mechanism Meet the Requirements of the Final Rule.

The Program Requirements and applicable assessment mechanism meet and exceed the requirements of sec. 312.10. The Program Requirements were modeled on the Organization for Economic Co-Operation and Development's ("OECD") principles of fair information practices, COPPA, and the requirements enunciated in the Final Rule. The Program Requirements were drafted to mirror sec. 312.2 through sec. 312.9 of the Final Rule. Therefore, member companies participating in the Children's Privacy Compliance Program are assured that by implementing the Program Requirements they are providing the same or greater protections for children as those contained in the Final Rule.

Specifically:

Section 312.2 (Defined Terms) - The Children's Privacy Compliance Program ensures that all defined terms described in sec. 312.2 of the Final Rule are adhered to because the Final Rule's definitions have been incorporated by reference into the Membership Agreement. As a result, member companies participating in the Children's Privacy Compliance Program are required to read the Program Requirements in a manner that is consistent with
sec. 312.2 of the Final Rule.

Section 312.3 (General Requirements) - Under sec. 312.3, the Final Rule sets forth the overall scheme of 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 notice 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 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, delete it, 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 company'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 company's information collection, use , and disclosure practices with regard to 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): Member companies must obtain verifiable consent before any collection, use, disclosure of personal information from children unless permitted to collect the child's first name or online contact information under one of the exceptions to prior verifiable parental consent set forth in sec. 312.5(c) of 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, 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.
The age information on the registration form 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;

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 they comply with their information policies and practices.

Section 312.4 (Notice) – The Program Requirements meet the Final Rule's requirement under sec. 312.4 that an operator of a website directed to children post a link to a notice of its information practices with regard to children on the homepage of its website and at each area on the website where personal information is collected from children. The notice of the member company's information practices must be clear and understandable, and should not contain unrelated, contradictory, promotional, or confusing material.

Specifically, the Program Requirements mandate that member companies post a privacy policy that states: (i) the notice of last update date to the privacy policy (ii) the member company's contact information; (iii) the types of personal information collected by the member company; (iv) how the member company uses the personal information; (v) whether the member company discloses personal information it obtains from the child; (vi) what form of control the parent or child has over their personal information; (vii) any restrictions on information collection that member companies must abide by when participating in the program; (viii) how a parent or child can access and review their information; (ix) the security and data protection employed to protect personal data; and, (x) where a parent or child can submit a question or complaint to the member company or to the Children's Privacy Compliance Program about its website's information policies or practices.

In addition to the seven program requirements that member companies must follow when participating in the Children's Privacy Compliance Program, each member company must also adhere to the provisions of the Membership Agreement that regulate the size, location and operation of the privacy policy link, These requirements are described in detail in the Membership Agreement.

Section 312.5 (Prior Verifiable Parental Consent) – The Program Requirements meet the Final Rule's requirement under sec. 312.5. Specifically, under Requirement 3 (A) of the Program Requirements, member companies must obtain verifiable parental consent before any collection, use, or disclosure of personal information from children. Member companies must also obtain such consent to any material change in the collection, use, or disclosure practices to which the parent has previously consented.

Moreover, under Requirement 3 (B), member companies must obtain prior verifiable parental consent. Such methods to obtain prior verifiable parental consent may include: (i) providing a consent form to be signed by the parent and returned to the member company by postal mail or facsimile; (ii) requiring the parent to use a credit card in connection with a transaction; (iii) having a parent call a toll-free telephone number staffed by trained personnel; or (iv) using one of the online or offline verification methods of the Integrity System.

The Integrity System is 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 verifiable permission. 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) the use of a credit card in connection with a transaction; (iv) email with an electronically signed parental consent form, and verification of an attached copy of a government-issued identity document (e.g., voter registration card, driver's license, other official license); (v) email with an attached 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 copy of a government-issued identity document; (vii) the electronic submission through a secure website (upload) and verification of an attached copy of a physically signed parental consent form; (viii) electronic transmission and verification of a photocopy of a government-issued identity document through Multimedia Messaging Service ("MMS"); (ix) electronic transmission and verification of a photocopy 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 identity document 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; 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.

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 away from all other corporate data. All Personal Identity Document numbers ("PID numbers") submitted during this process (*e.g.*, SSN4, Driver's License Number, Passport number) shall be stored in a secure encrypted form immediately after submission, and all such PID numbers shall be deleted a reasonable time after submission. Should new rules be adopted to require immediate deletion of any information, such change will be implemented.

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 no other.

The Integrity System is an efficient and effective means for a parent to give permission to a member company's website that wishes to collect personal information from the parent's child. In most cases the online or telephone verification process only takes a few minutes to complete; the offline method of faxing may take 1 day; the offline method of mailing may take from 3- 5 days.

The need for parental consent is triggered when the child first attempts to register at the website and is immediately greeted by a "gate" in which he/she must provide their birth date. Upon entering information that indicates the child is under 13, the child provides the parent's information so the member can contact the parent. .

At this point the parent begins the verification process. The first step is for the parent to register with the website. Prior to completing the adult registration form, the parent will be given notice via the direct notice email of the website's information collection, use, and disclosure practices with regard to the child in accordance with Requirement 2 of the Program Requirements and COPPA. Once the parent has read the Direct Notice to Parent, the parent is prompted to complete the adult registration.

The next step is to verify that the individual providing consent is an adult by one of the methods of verification mentioned above. In the event that the Parent has been verified through one of these methods of verification mentioned above, a Parent may authorize a subsequent sibling through an electronic authorization either through e-mail, fax, mail or electronic acknowledgement that confirms the relationship of a subsequent sibling as part of that family.

If the parent successfully verifies using one the methods described above, the parent will then be able to provide consent for the account that their child has already initiated or, if the parent has not registered their child but would like to, set up a new account for their child. The parent will also be able to actively manage their child's account information, including what website features their child can participate in or whether they can receive information such as newsletters from the member company.

Furthermore, where a website is solely directed to children 12 years old or under and does not provide a "gate" where the individual must provide his or her birth date, a member company must assume that the individual is a child and obtain verifiable consent from that individual's parent before collecting, using, or disclosing the child's personal information.

Lastly, even though prior verifiable parental consent is required under most situations before a member company is permitted to collect use, or disclose a child's personal information, there are a few exceptions where a member company is permitted to collect a child's first name or online contact information before obtaining consent from the child's parent. In such circumstances, member companies must comply with Requirement 3 (C) of the Program Requirements, which describes the exceptions to prior verifiable parental consent and is consistent with the Final Rule's requirement under sec. 312.5(c).

Consistent with sec. 312.5 of the Final Rule, member companies are also required to give the parent 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.

Section 312.6 (Right of Parent to Review Personal Information Provided by Child) - The Program Requirements meet the Final Rule's requirements under sec. 312.6, which states that upon request of a parent whose child has provided personal

information to a website that such website provide the parent with an opportunity to access and review their child's personal information Specifically, under Requirement 4 of the Children's Privacy Compliance Program, member companies are required to provide parents with the ability to access and review their child's personal information. Parental access and review must consist of: (i) a description of the specific types of personal information collected from the child; (ii) the opportunity at any time to refuse to permit the company to further use or collect the child's personal information; and (iii) the ability to direct the company to delete the child's personal information from the company's records.

Section 312.7 (Prohibition Against Conditioning Child's Participation on Collection of Personal Information) – The Program Requirements meet the Final Rule's requirements under sec. 312.7, prohibiting an operator of a website from conditioning a child's participation on collection of personal information. The Children's Privacy Compliance Program recognizes that many websites may require a child to provide their personal information to participate in activities on the website such as games, contests, or sweepstakes. And although the Children's Privacy Compliance Program does not limit such practices, member companies are required to restrict the amount of information they collect about the child.

Specifically, under Requirement 5 of the Children's Privacy Compliance Program, member companies 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, Member companies must also continually re-evaluate whether a valid reason exists for the information to be collected. And if the valid reason ceases to exist, member companies must restrict their collection practices in view of their revised business model.

Section 312.8 (Confidentiality, Security, and Integrity of Personal Information Collected from Children) - The Program Requirements meet the Final Rule's requirements under sec. 312.8 by mandating that all member companies establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. For example, member companies must implement internal security measures that protect the confidentiality of the child's personal information and protect such information from loss, misuse, unauthorized access, or improper disclosure.

Section 312.9 (Enforcement) - The Children's Privacy Compliance Program compliance and enforcement mechanisms meet the Final Rule's requirements as enunciated in sec. 312.9. Member companies are required to institute internal control mechanisms. Specifically, these mechanisms include appointing a representative of the member company that is responsible for handling all questions or complaints received from parents or children that use its website. Such representative must be given the full authority to receive and actively respond to any privacy-related inquiries. If a member company has not adequately responded to a parent's or child's inquiry, the member company must provide a means for the parent or child to appeal to a higher management level. In the event the parent or child remains unsatisfied with the member company's response, the member company is required to refer the parent or child to the Children's Privacy Compliance Program.

In addition to these internal control mechanisms, the Children's Privacy Compliance Program also requires member companies to adhere to Requirement 7. Under the Compliance and Enforcement Requirement, member companies agree to submit to compliance monitoring and shall cooperate in all respects with the Children's Privacy Compliance Program monitoring of the member company compliance with the terms and conditions set forth in the Membership Agreement.

Moreover, member companies must provide the parent and the child with reasonable and effective means to submit complaints that they may have about a member company's information practices. The Children's Privacy Compliance Program compliance and enforcement mechanisms are discussed in further detail below.

III (B) HOW THE ASSESSMENT MECHANISM AND COMPLIANCE INCENTIVES REQUIRED UNDER SECTION 312.10(B) (2) AND (3) PROVIDE EFFECTIVE ENFORCEMENT OF THE REQUIREMENTS OF THE FINAL RULE.

Mandatory mechanism for the independent assessment of a subject operator's compliance with the guidelines – The Children's Privacy Compliance Program meets the requirements of sec. 312.10 (b) (2) of the Final Rule. Section 312.10 (b) (2) states that an effective, mandatory mechanism for the independent assessment of a member company's compliance with the Program Requirements is required. The Children's Privacy Compliance Program accomplishes this requirement in a number of ways, including the following:

Initial and Annual Self-Evaluation - Member companies must conduct an evaluation of their website's information collection, use and disclosure practices, Each member company is required to complete and attest to the accuracy of the statements it

makes on a self-evaluation form about its information practices, Once the member company sends the self-evaluation form to the Children's Privacy Compliance Program, a representative of the Children's Privacy Compliance Program will independently review the self-evaluation form in conjunction with the website's actual practices to make sure what is stated in the self-evaluation form is consistent with such practices and the Program Requirements. See Monitoring Form, Exhibit B.

The independent review will consist of three steps. The first step is for a trained privacy monitor to systematically evaluate the responses made by the member company in its self-evaluation form, one question at a time, with the notice and disclosure statements contained in its posted privacy policy Any inaccuracies found in the privacy policy must be modified to accurately reflect the member company's actual information practices before the Children's Privacy Compliance Program will issue a Seal of Approval for that particular website.

The second step is for a trained privacy monitor to review the member company's website and compare the website review with the member company's self-evaluation form and posted privacy policy to ensure that the privacy policy accurately depicts the collection practices of the website.

The third step is for a trained privacy monitor to conduct a review of the website's information collection and use practices. During this segment of the website review process, a privacy monitor will submit fictitious personal information at each point within the website where information is collected and then track that information to determine whether the member company is using the personal information it has obtained in conformity with its stated privacy policy. If personal information is collected from children twelve years old or under, then the privacy monitor verifies that prior verifiable parent consent is obtained before the child's personal information is collected by the website.

In the event the member company's 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. To ensure that member companies remain in full compliance, each member must submit to the procedures described above on an annual basis. This allows the Children's Privacy Compliance Program to make sure that the website is in full compliance with Program Requirements and COPPA before renewing the website membership in the Children's Privacy Compliance Program for an additional year.

Compliance Monitoring - Member companies must submit to quarterly and periodic, unannounced monitoring reviews of their website information practices. The purpose of these monitoring reviews is to ensure that a member company's privacy policy is consistent with its website information practices. Monitoring reviews also allow the Children's Privacy Compliance Program to verify that the member's website complies with the Program Requirements and COPPA at all times.

All member companies must submit to quarterly monitoring reviews of their website information practices. These monitoring reviews will be conducted at a minimum of once per quarter or four times per year. Specifically, monitoring reviews are conducted by trained privacy monitors that systematically move about a member company website ensuring that: (i) there is prominent link to the website privacy policy on the homepage and any web page where information is collected by the website; (ii) the member company obtains prior verifiable parental consent from all children twelve years old and under before collecting their personal information; and (iii) there is compliance with the Program Requirements.

In addition to the quarterly monitoring, member companies must also agree to submit to periodic, unannounced monitoring reviews of their website. These periodic, unannounced reviews will be used to further verify that the member company remains in full compliance with the Program Requirements. During these monitoring reviews, the Children's Privacy Compliance Program randomly checks each participating website privacy practices.
These random checks are similar to the reviews done during the quarterly monitoring with the additional element of "seeding". As mentioned previously, the Children's Privacy Compliance Program will also periodically "seed" the personal information the member company website has collected. In other words the privacy monitor will submit fictitious information into its database that it maintains on behalf of a member company to track how the member company uses the personal information it has collected. These periodic reviews are another way that the Children's Privacy Compliance Program can insure that the member company is adhering to its website's posted privacy policy.

Reviews are memorialized in written reports provided to the member and maintained by the Children's Privacy Compliance Program for a period of at least three (3) years.

Consumer Complaints/Monitoring – Member companies must provide the parent and the child with reasonable and effective means to submit complaints that they may have about a member company's information practices. The Children's Privacy Compliance Program also offers the parent or child the opportunity to submit complaints about any member company directly to the Children's Privacy Compliance Program. A Children's Privacy Compliance Program representative responds to all complaints immediately.

Effective incentives for subject operator's compliance with the guidelines – Section 312.10(b) (3) of the Final Rule requires the Children's Privacy Compliance Program to provide effective incentives for member companies to ensure full compliance with the Program Requirements. This requirement is met in the following manner:

Membership Agreement Obligations - Member companies must execute the Children's Privacy Compliance Program membership agreement. As part of this agreement, member companies must agree to comply with these Program Requirements at all times. In the event that a member company 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.

Consumer Complaints/Monitoring – Each member company shall create and implement effective and affordable mechanisms that ensure compliance with its Privacy Policy and provide appropriate means of resolving consumer complaints. Such mechanisms for resolving consumer complaints include the appointment of at least one individual to whom a parent or child can bring inquiries regarding member company privacy practices The designated individual must be given the authority by the member company to investigate all inquiries or complaints and complete this investigation in a timely manner, but in no event later than fourteen (14) business days.

The member company is required to cooperate with the Children's Privacy Compliance Program efforts to resolve complaints, questions, and concerns on behalf of a parent or child. In the event a parent or child is not satisfied with the means of recourse provided by the member company and/or the resolution of a complaint, the member company is required to refer the individual to the Children's Privacy Compliance Program.

If the Children's Privacy Compliance Program determines that a violation of the requirements has occurred, the member company is informed of such violation and the corrective actions that must be taken to bring the member company website into compliance. Failure to take the corrective actions can result in a number consequences, including removal from the Children's Privacy Compliance Program (as described above under Membership Agreement obligations) and referral to the appropriate governmental agency (as described below under Referral to the Commission).

Member companies must maintain records for a period of at least three (3) years of all complaints, concerns, or inquiries received about its website and any responses to the consumer addressing such complaint or concern.

Referral to the Commission –If the Children's Privacy Compliance Program determines, after a thorough investigation into the member company's information practices, that a member company has violated its posted privacy policy or any of the Program Requirements, the Children's Privacy Compliance Program is prepared to refer such member company to the Commission for possible unfair and deceptive trade practices.

IV. CONCLUSION

It is our belief that the Integrity Children's Privacy Compliance Program, the Membership Agreement, the Compliance and Enforcement mechanisms, the Integrity System, and the individualized counseling we make available to member companies will provide an effective self-regulatory program for protecting the personal information of children online.

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

(Proprietary: To be Redacted From Public Record Version)

EXHIBIT A TO **INTEGRITY CHILDREN'S PRIVACY COMPLIANCE PROGRAM MEMBERSHIP AGREEMENT**

INTEGRITY CHILDREN'S PRIVACY COMPLIANCE PROGRAM REQUIREMENTS

EXHIBIT A TO **INTEGRITY CHILDREN'S PRIVACY COMPLIANCE PROGRAM MEMBERSHIP AGREEMENT**

INTEGRITY CHILDREN'S PRIVACY COMPLIANCE PROGRAM REQUIREMENTS

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.

Definitions

"Personal Information" means individually identifiable information about any individual collected online from a child under 13, 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) an email address or other online contact information, including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security number; (f) a persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or (g) information concerning the child or the parents of that child that the operator collects online from the child and combines with any individually identifiable information described in this definition.

Requirement 1: Notice/Disclosure of Information

Members with online activities that are directed at children under the age of 13, or that have actual knowledge that they are collecting or maintaining personal information from children under the age of 13, 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, must display the Children's Mark and must abide by this Exhibit A, Children's Program Requirements, as set forth herein. If a section of Member's Site is directed at children under 13, Member must display Aristotle's Children's Mark on that section of the Site and must abide by this Exhibit A.

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 located 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 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 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. If using a hypertext link, the text must have a 10-point minimum font size or be consistent with the size of the other menu items, whichever is larger. 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 must 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. See also http://privacy.integrity.aristotle.com/downloads/coppa-how-comply.pdf for guidance on privacy policy requirements. 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. In cases where more than one company is responsible for a website, the Member may choose to respond to all inquiries from parents concerning the Member privacy policies, provided that the names, physical addresses, telephone numbers, and email of all persons or companies collecting personal information through the website are listed in the privacy policy.

C. Types of Personal Information Collected: Members must describe the types of personal information collected 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) whether the third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the Member; and (3) 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; and (4) identify and provide information (name, physical address, telephone number, and email address) concerning any third party that is collecting personal information through the member website or with whom the member is sharing such information.

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. Restrictions on Information Collection: Members must state that they 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.

H. Access to Information: 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 to access their child's personal information.

I. Data Security and Protection: Members must state specific information disclosing the manner in which that Member intends to protect personal information (e.g. use of SSL, firewalls, other encryption methods, etc.).

J. 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

Members must make reasonable efforts to ensure that a parent of a child receives notice of the Member's information collection, use, and disclosure practices with regard to children, including notice of any material change in the collection, use, or disclosure practices to which the parent had previously consented. Mechanisms to provide notice include, but are not limited to, sending the notice to the parent's email address or sending the notice by postal mail.

Direct Notices to Parents must contain the following information:

A. Privacy Policy Information: Members must include all of the information that is necessitated as part of Requirement 1 above.

B. Purpose is to Collect Information: Members must state that they wish to collect personal information from the child.

C. Parental Consent Required: Members must state that the parent's consent is required for the collection, use, or disclosure of the child's personal information. Members must also describe the method by which a parent may give such consent.

Except for certain circumstances described below under Requirement 3(C), Members must meet the requirements described above and obtain prior verifiable parental consent before they are allowed to collect personal information from children.

Requirement 3: Prior Verifiable Parental Consent

A. Generally: Members must obtain verifiable parental consent before any collection, use, display, or disclosure of personal information from children under 13, and will make best efforts to prevent a child from doing so 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 Section 3(B) 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 may be subject to a revision fee.

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 section 3(A) 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. 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 Member by postal mail or facsimile; (ii) requiring the parent to use a credit card in connection with a transaction; (iii) having a parent call a toll- free telephone number staffed by trained personnel; or (iv) 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 verifiable permission. 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) the use of a credit card in connection with a transaction; (iv) email with an electronically signed parental consent form, and verification of an attached copy of a government-issued identity document (e.g., voter registration card, driver's license, other official license); (v) email with an attached 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 copy of a government-issued identity document; (vii) the electronic submission through a secure website (upload) and verification of an attached copy of a physically signed parental consent form; (viii) electronic transmission and verification of a photocopy of a government-issued identity document through Multimedia Messaging Service ("MMS"); (ix) electronic transmission and verification of a photocopy 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 identity document 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; 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.

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 away from all other corporate data. All Personal Identity Document numbers ("PID numbers") submitted during this process (*e.g.*, SSN4, Driver's License Number, Passport number) shall be stored in a secure encrypted form immediately after submission, and all such PID numbers shall be deleted a reasonable time after submission. Should new rules be adopted to require immediate deletion of any information, such change will be implemented.

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 no other.

C. Exceptions to Verifiable Parental Consent: Even though verifiable parental consent is required under most situations before a Member is permitted to collect, use, or disclose a child's personal information, there are a few exceptions where a Member will be allowed to collect a child's first name or online contact information before obtaining consent from the child's parent. The exceptions to prior verifiable parental consent are as follows:

- *Required Parental Consent* - Members may collect the first name or online contact information of a child to be used for the sole purpose of obtaining the parental consent. If a 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. Members that collect the first name or online contact information from a child under this exception must provide direct notice to the parent. The direct notice must include all privacy policy information (*See* Requirement 2 (A), above) and notify the parent that the Member has collected the child's first name and email address to respond to and obtain consent from the parent. If the Member has not obtained parental consent after a reasonable time from the date the information is collected, the Member must delete such information from its records.

- *One-Time Request* – Members may collect the online contact information of child for the sole purpose of responding directly, on a one-time basis, to a specific request from the child. Members that collect the online contact information from a child under this exception must not use the information to recontact the child after the initial response and must delete the child's personal information. Direct notice is not required under this exception.

- *Multiple Requests* – Members may collect the online contact information from a child to be used to respond directly more than once to a specific request from the child so long as the information is not used for any other purpose. Members that obtain the online contact information from a child under this exception must provide direct notice to

the parent. The direct notice must: (1) include all privacy policy information (*See* Requirement 2 (A), above); (2) notify the parent that the Member has collected the child's online contact information to respond to the child's request; (3) explain the nature and intended use of the information; (4) inform the parent that they may request that the Member make no further use of the information and that such information be deleted; (5) describe the procedures by which the parent can refuse to allow further contact and information collection from the child; and, (6) explain that if the parent does not opt out, the Member may use the information for the purposes stated in the direct notice. The direct notice must be sent after the initial response and before making any additional response to the child.

- *Child Safety* - Members may collect the child's first name or online contact information to the extent reasonably necessary to protect the safety of a child participant on the website where the Member used reasonable efforts to provide notice to the parent. The information collected by Member under this exception must be used for the sole purpose of protecting the child's safety, must not be used to re-contact the child or for any other purpose than for the purpose stated in this exception and must not be disclosed by a Member on its website. The direct notice must: (1) include all privacy policy information (*See* Requirement 2(A), above); (2) notify the parent that the Member has collected the child's online contact information to protect the safety of the child participating on the website; (3) inform the parent that they may refuse to permit the use of the information and may require its deletion, and inform them how they can have the information deleted; and, (4) explain that if the parent does not opt out, the Member may use the information for the purposes stated in the direct notice.

- *Additional Safety Concerns* - Members may collect a child's first name or online contact information to protect the security or integrity of the website, to take precautions against liability, to respond to judicial process, or to provide information to law enforcement agencies or 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.

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

Members must provide parents with the ability to access and review their child's personal information. Parental review and access must consist of: (a) a description of the specific types of personal information collected from the child; (b) the opportunity at any time to refuse to permit the Member from further using or collecting the child's personal information; and (c) the ability to direct the Member to delete the child's personal information from the Member records.

In addition to providing the ability for a parent to access and review their child's personal information, Members must take reasonable steps to ensure that the individual requesting access is the child's parent. Acceptable steps for authenticating the identity of the individual online include a username and password unique to the individual or, if access is requested over the telephone, asking a series of questions that only a parent of the child would have knowledge of (e.g., parent's name, mailing address, email address, child's name, child's email address, etc.).

Requirement 5: <u>Restrictions on Information Collection</u>

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.

The age information on the registration form 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;

Requirement 6: <u>Confidentiality, Security and Integrity of Information</u>

Members must disclose their data retention and deletion policies/practices and only retain data that is necessary for ongoing business operations.

Members must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. 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 will be conducted on a quarterly basis. In addition to the quarterly 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.

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

Verification Page Text

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

Verification Page Text

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]

Appendix 2 to Integrity Children's Privacy Compliance Program Membership Agreement

(To be Redacted From Public Record Version)

Integrity Children's Privacy Compliance Program

Self-Evaluation Review Report

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

Sample Marks

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

Sample Marks

Graphical user interface 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

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 312.10 of the Children's Online Privacy Protection Rule.

Integrity Privacy Compliance Program

Monitoring Review Report

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 312.10 of the Children's Online Privacy Protection Rule.

Integrity Privacy Compliance Program

Monitoring Review Report

Website Name: _____

Website URL: _____

Company Name: _____

Contact Name: _____

Date Reviewed: _____

PRIVACY POLICY:

1. **Does the website have a prominent privacy policy link displayed on its homepage?**

   0 Yes 0 No

2. **Does the privacy policy link take the users to the website's privacy policy?** 0 Yes 0 No

3. **Is a privacy policy link displayed on all web pages where personal information is collected?**

0 Yes 0 No

4. **Does the website's privacy policy include the following information? Please place a check next to the information contained in the website's privacy policy and attach a copy of the website's privacy policy to this report.**

[] Company's complete contact information

[] Types of personal information the website collects

[] How the website will use the information it collects

[] How the website discloses the information that it collects

[] The choices available to the parent and child with regard to how their personal information may be used

[] Whether the website prohibits the 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 necessary

[] How the child can access his or her personal information

[] How the parent can review the child's personal information[] How the parent can delete the child's personal information

[] How the parent stop further collection of the child's personal information

[] Where the parent or child can address any questions or complaints that they may have regarding your website

5. **Is the privacy policy reconciled with Terms of Use, Terms of Service or End User License Agreement?** 0 Yes 0 No

<u>WEBSITE</u>:

1. **Does the website collect personal information from children under 13?** 0 Yes 0 No

2. **What types of personal information does the website collect from the child or the parent of that child?**

[] First name

[] Last name

[] Mailing address

[] Email address

[] Telephone number

[] Credit card number and expiration date

[] Last four digits of the parent's social security number

[] Other, please explain further:_____

_____

3. **Does the website request parental consent before obtaining personal information from children under 13?** 0 Yes 0 No

4. **Does the website utilize an age-gate?** 0 Yes 0 No
If so, is the language age-neutral? 0 Yes 0 No

5. **Does the website utilize cookies to prevent back-buttoning?** 0 Yes 0 No

6. What method of parental consent does the website employ?

[] Sign, print, and send method

[] 800-Number supported by trained personnel

[] Aristotle Integrity System

[] Other, please explain further:_____

_____

7. Does the website provide Direct Notice to Parents at the time they obtain parental consent? 0 Yes 0

8. What type of information does the Direct Notice to Parents contain?

[] All information contained in the privacy policy

[] A statement notifying the parent that the website wishes to collect personal information from the child and cannot do so without prior verifiable parental consent

[] A statement that the parent can consent to the website's collection and internal use of personal information without consenting to the disclosure of that information to third parties

[] A statement about how the parent can limit disclosure of their child's personal information

9. Does the website collect demographic information? 0 Yes 0 No (If yes, please select all that apply):

[] Username and password

[] Date of birth or age

[] Gender

[] Hobbies and interests

[] Other, please explain further:_____

_____

10. **Does the website feature message boards, chat rooms, or other interactive features where a child's personal information can be publicly disclosed?** 0 Yes 0 No

Please describe the types of interactive features contained on the website:

_____

_____

_____

_____

_____

11. **Does the website use passive collection mechanisms?** 0 Yes 0

12. Which passive collection mechanisms does the website use?

[] Cookies

[] Clear GIFs

[] Other, please explain further:_____

_____

13. Does the website link to other websites on the World Wide Web? 0 Yes 0

14. Does the website include a bumper screen or a notice that warns the user that they are leaving the current website and that the website's privacy policy no longer applies? 0 Yes 0 No

15. Does the website provide the parent or the child with the ability to make a choice about how their personal information will be used? 0 Yes 0 No (If yes, please indicate what type of choices)

What type of choice does the website offer?

[] The website offers users the opportunity to opt-out of an activity or from receiving information

[] The website offers users the opportunity to opt-in to an activity or to receiving information from our company or other permitted entities

[] The website offers users with either the opportunity to opt-in or opt-out depending on the activity

[] Other, please explain further:_____

_____

16. Please describe any general concerns or comments about the website:

_____

_____

_____

IF YOU ARE CONDUCTING A PERIODIC, UNANNOUNCED MONITORING REVIEW, PLEASE FOLLOW THE DIRECTIONS BELOW:

SEEDING INFORMATION:

Please complete all registrations or forms on the website. The privacy monitor will provide you with the necessary fictitious information, including the name, address and email address.

Insert the fictitious information used during your monitoring review session in the space

provided:

Child's Name: _____

Child's Email Address: _____

Parent's Name: _____

Parent's Email Address: _____

Mailing Address: _____

_____
