The Advertising Research Foundation Member Code of Conduct

February 2019

Who We Are

The ARF was formed in 1936 as a non-profit foundation committed to introduce and support the scientific practice of advertising and marketing research. Over the years, it has taken the leadership position in the industry as a platform for conducting, publishing and presenting research that advances the advertising and marketing industry.

The ARF is unique relative to its many partner associations in that it is not an advocacy group for any one sector of the advertising industry. Its 400+ members include advertisers, advertising agencies, adtech and martech companies, consultants, media and research companies. This is a great advantage in that it assures its independence in judgement and research interpretation. It does represent some special requirements in fashioning a Code of conduct that reflects such differences in members' business models.

Therefore, in Part I, we present a set of general member principles established for all members and in Part II, principles relevant to specific member industry sectors.

PART I
General Member Principles

The Code, as it applies to all members, covers a member's responsibility to research participants, clients (both internal and external), and, to the profession and the public. These general principles fall under four broad classes: Honesty, Integrity, Transparency and Implementation via a Chain of Trust. The "public" refers to all those who may receive unsolicited "*contacts"*, including those receiving research instruments, advertising, marketing messages, e-commerce messages and other forms of communication.

The scope of this Code covers all aspects of research, modeling, analytics and segmentation whether by human hand or automated. The scope does not extend to cover the process of activation or targeting itself.

Part I. A: Responsibilities to Research Participants

While the ARF membership is composed of Advertisers, Agencies, Media, Ad Tech, Marketing, Consultancies and Research companies, this first section is focused on research participants. As such, it is closely aligned with the ICC/ESOMAR International Code.

https://www.esomar.org/uploads/pdf/professional-standards/ICCESOMAR_Code_English_.pdf

1. The Principle of Honesty

A. Participation in research must be voluntary
   i. Ensure participants understand the purpose of the research, the anticipated length and what is expected of them
   ii. Participants have the right to terminate at any point in the research
   iii. Collect PII only with participant knowledge and consent
   iv. State whether the participant will be re-contacted for any purpose, why and when

2. The Principle of Integrity

A. Misleading or deceptive practices must not be used
   i. Hidden identifiers must-not be used
   ii. Participants must be told If responses are not anonymous
   iii. Participants must be told if their responses are being monitored by the sponsoring client
   iv. No false or misleading information is used such as addresses, emails, brand names or companies. If a Placebo brand or company is needed for the research, the participant should be debriefed after the research
   v. Do not represent selling, fundraising or any non-research activity as research
   vi. Obtain consent before using data in a manner materially different from the original purpose
   vii. Inform participants of audio / visual recording prior to the initiation of recording

B. Research participants shall come to no harm, harassment or direct action based on the decision to participate or not participate in the research.
   i. Empirically support a policy on the number of callbacks or contacts
   ii. The number of callbacks should balance response rates against the perception of harassment
   iii. Validation must balance quality with intrusiveness
   iv. Sample providers should identify the process by which the sample was recruited
   v. Data are not to be used for targeting or other non-research purposes without participant consent

C. Use best practice methods to protect the privacy and PII of all participants
   i. Protect privacy and interests of children, young people, and other vulnerable populations by complying with COPPA and HIPAA laws
   ii. Allow participants to access, correct or update any PII held about them
   iii. Share PII with a third party only with explicit consent
   iv. Identify if PII is to be shared with Affiliated Companies
   v. Limit data collection to what is essential for the research objective
   vi. Passively collected data such as mobile location, voice, text, browser activity, apps and email must be de-identified

3. The Principle of Transparency

A. Privacy policies should be readily available
   i. Online surveys must link to a privacy policy
   ii. Privacy policies should be clear, concise, and easy to understand
   iii. Policies should describe the choices participants have, whether other companies will receive deidentified or identified data, who has access and for what purpose
   iv. Policies should identify compliance with relevant privacy laws
   v. As will be noted throughout this Code, members should monitor the use and comprehension of their privacy policies with an objective of continuous improvement

B. Provide the name of the research organization and affiliated parties conducing the research so that if the respondent wants to contact the research company for any reason, they have legitimate contact details

   i. The client or sponsor will be disclosed during or at the end of the research. However, there are cases where such

disclosure might inform the public about confidential information such as product development plans. Another exception might be when knowing the sponsor might affect the responses. In such cases, the researcher should find a deliberate balance between full transparency and the protection of confidential information by using more general descriptors such as ”a major retailer” or “a major automotive company”

4. The Chain of Trust Principle

One objective of creating and committing to a comprehensive Code of conduct is to create an ecosystem that can credibly self-regulate. Members who commit to this Code may display the ARF Code logo on correspondence and marketing materials. Members who violate the Code will be asked to remove the logo from all materials. However, real enforcement that supports self-regulation comes in the form of a Chain of Trust which tells clients that the industry partner they have engaged, has committed to the principles expressed in this Code and has asked all other parties in the project chain to make the same commitments.
.

Member companies should have one person who owns the responsibility of adherence to this Code. We recommend this be the member ambassador. To adhere to the Code, the member ambassador must submit an annual statement certifying that the member organization has used reasonable efforts to apply the Code and has communicated the Code to the appropriate people in the organization. This communication may take the form of email to the executive team or those operating in the privacy space as it applies to the research function and/or posting in a visible location not unlike the posting of employment laws in common areas.

Implementation, enforcement and probationary member status is covered under a separate memorandum: The ARF Code of Conduct Implementation Procedures. The ARF is likely to update these procedures more frequently than the Code itself and therefore it lives as a separate memorandum.

Part I.B: Responsibilities to Clients

1. The Principle of Honesty

A. Engage in honest statements of work (SOW) and contract agreements with business partners
   i. Study designs, modeling processes, ad channels, targeting segments, campaigns and other work product should be demonstrably fit for use given the client’s objectives
   ii. If asked, fit for use can be empirically demonstrated

2. The Principle of Integrity

A. Document all work to be completed and confidentiality requirements
   i. The SOW or business agreement must clearly state
      a. Who owns the work product
      b. How, when and where the work product and KPIs are made public or are confidential
   ii. Clients must approve if work product will be combined with other data or data collection
   iii. Clients must approve if work will be subcontracted
   iv. All data, lists, flowcharts, copy and other materials provided by a client remain the client’s property
   v. Do not use data collected for one client for another without permission
   vi. Ensure project materials are retained or disposed of according to the SOW and the law. One such law may be found at: https://www.ftc.gov/news-events/media-resources/truth-advertising
   vii. Comply with all obligations and limitations of use by data owners when purchasing data or sample
   viii. Keep confidential all information about clients’ business, business strategy and any proprietary measures and frameworks developed with or by the client

3. The Principle of Transparency

A. Inform client of all quality control and validation KPIs
   i. If requested, allow client to monitor projects in progress as long as it does not affect the results or interfere with respondent privacy
   ii. Allow for client and/or independent assessment or validation
   iii. Ensure programmatic clients understand all measures and limits to the protection of brand safety
B. Where sample is used, a clear transparent statement of what the sample represents must be provided
C. Suppliers will also supply clients with timely notice when schedules or deliverables listed in the statement of work are comprimised

4. The Chain of Trust Principle

As with all responsibilities, the Chain of Trust ensures clients that the industry partner they have engaged has committed to the principles expressed in this Code and has asked all other parties in the project chain to make the same commitments.

Part I.C Responsibilities to the Profession and the Public

1. The Principle of Honesty

A. Must avoid the use of harassment or misleading recruiting and sampling techniques
B. When data or reports are made public, ensure that:
   i. A client release is consistent with the results provided
   ii. The public can request non-confidential technical information about the underlying data in order to evaluate the veracity of the public claims
C. When online behavioral, interest or location data are used to *contact* individuals for any reason, privacy statements will state explicitly what is collected, how it is collected, how it is used and with whom it is shared. Contacted individuals should have an easy way to opt-out
   i. Online behavioral or interest data may include but not limited to text, voice, search, social media and web browsing
   ii. Location data includes that which is passively collected through mobile apps and other technologies
   iii. See also the DAA guidelines for non-research related reasons:

Self-Regulatory Principles for Online Behavioral Advertising

2. The Principle of Integrity

1. Comply with all applicable laws and regulation
   i. These include data privacy laws and also commitments via terms of service agreements and privacy policies
   ii. Abide by all protections of vulnerable populations including those under COPPA and HIPAA
      a. Members should consult the Children's Advertising Review Unit guideline administered by the Better Business Bureau

http://www.asrcreviews.org/wp-content/uploads/2012/04/Self-Regulatory-Program-for-Childrens-Advertising-Revised-2014-.pdf

   iii. Observe all licensing restrictions

B. Do not engage in illegal anti-competitive behaviors
   i. Respect confidentiality statements especially those captioned on competitor's documents

C. Members will treat PII in strict accordance with their privacy policies and those expressed in this Code
   i. Members will adhere to the same Principles of Integrity expressed in section I.A.2. A-C, Responsibilities to Research Respondents
      a. Allow the public to access, correct, or update any PII held about them
      b. Gain consent before sharing PII with a third party
      c. Limit data collection to what is necessary for the specific project purposes

D. Members should identify what they consider PII.
   i. PII today goes well beyond name, address and phone. Data that can support the de-anonymization of anonymized data should be considered PII
   ii. Members should consult the current FTC definitions for guidance
   iii. Members should use custom or shared research to determine what the public considers sensitive data and use that research to consider what it considers PII or restricted data
      a. The ARF has conducted research on the public's comprehension of certain phrases. This is an example of shared research that could be used to improve a policy statement
   iv. Members should explicitly state if they consider digital IDs PII
E. Members that take privacy seriously should study time spent and monitor other KPIs related to the terms of service or privacy policy with an objective of continuous improvement
F. Whether using primary results or available data sets, there must be intellectual honesty in conclusions and interpretation of results

3. The Principle of Transparency

A. When online behavioral, interest or location data are used to contact or target individuals for any reason within the scope of this Code, members will use custom or shared research to measure the extent to which the public understands the concepts expressed in a term of service or privacy policy
   i. That program may use secondary research conducted to develop best practices for features such as formatting or language use.
   ii. Members that use online behavioral, interest or location data will also regularly review and update their privacy policies with the intent of continuously improving the public's understanding of the member's terms of service

4. The Chain of Trust Principle

The Chain of Trust ensures the public that a company, with which they have a first-party relationship, will ensure that their privacy rights will be protected. If any data are shared up or down the chain, this protection must extend in a fashion as stated in that company's privacy policy or term of service. Members will only use data that has been ethically obtained, consistent with the ethics outlined in this Code.

Part II
Sector Specific Principles
Part II.A Online Behavioral/Interest/Location Based Research Contacts

The Digital Advertising Alliance (DAA) has established a set of principles upon which many companies in the digital advertising sector have based their data privacy policies. As such, this ARF Member Code of Conduct reiterates those principles as guidance for its members. Click here to view the DAA guidelines:

Self-Regulatory Principles for Online Behavioral Advertising.

ARF members should periodically review the DAA guidelinesfor updates.

1. Education

A. Members should support and/or conduct custom or shared research to determine whether consumers understand the member's terms of service and data privacy policy. This understanding should include:
   i. How digital behavioral/interest/location-based messaging works at a conceptual level
   ii. Where and what data are collected
   iii. Their options to limit data collection and use
   iv. Definitions of terms, such as "third parties" and "cookies," used in their privacy statements and
   v. What recourse consumers have in cases of violation of these principles

B. This should be done in the spirit of continuous improvement

2. Transparency

A. Members should state when and how they are using automated decision or artificial intelligence systems and provide a clear and easy opt-out ability
   i. Automated decision systems have been shown to have implicit biases based on the training data. When such systems are used, these biases should be studied, understood and minimized by:
      a. Limiting the types of data available
      b. Modifying the systems to counteract the biases
      c. Using interpretable systems which can explain the automated decision, or
      d. Using human in the loop systems where significant bias can be modified

B. Members using identity graphs across smart tv, return path data, phone, text, location, voice assistants, email, PCs and mobile should describe how these devices are linked, what data are collected, for what purpose and provide a clear and easy opt-out
   i. KPIs should include the number or percent of users who read and understand these statements

3. Consumer Control

A. This principle requires an easy way for consumers to withdraw consent for the collection and use of data
   i. Withdrawal of consent to collect and use data strongly suggests the consumer no longer wants that data retained. Except in cases where retention is required for legal purposes, withdrawal of consent should initiate consumer control allowing easy and clear access to and immediate deletion of the data
   ii. Account deactivation or deletion should initiate consumer control allowing withdrawal of consent

B. Implement or recognize an alternative method for consumers to opt-out
   i. State that clearing cookies or changing browsers negates the decision to opt-out
   ii. Requiring consumers to opt-out of each third party to which their information may be shared is an unreasonable task. Offer the use of one of the consent management platforms such as AdChoices to minimize this effort

Part II.B Neuro and Biometric Research

The Neuromarketing Science and Business Association (NMSBA) has published a comprehensive Code of ethics for the application of neuroscience in business. Many of the principles and articles expressed in this Code are captured in Part I, the ARF general member principles. However, we urge all members who conduct Neuro or Biometric research to commit to the NMSBA Code which can be found at

http://www.nmsba.com/Ethics .

Part II.C Users of Syndicated Research

A. Many forms of syndicated research are unique in that they are used as currency or to set value or as a performance measurement system

i. In the case of Media Research such as television ratings and digital impressions, no member shall attempt to influence the accuracy of the data
    a. Unethical attempts to influence syndicated data may include but are not limited to:
        i. Determining the location of panel households
        ii. Contacting panel households
        iii. Making in-market announcements intended to affect panelists
        iv. Using bots or other technologies to inflate impression counts or clicks
        v. Any method of digital fraud

ii. In the case of Syndicated Sales or Consumer Research which serves as a performance management measure
    a. Unethical attempts to influence sales or consumer data may include but are not limited to:
        i. Identifying sampled stores
        ii. Targeting special activities in those stores
        iii. Identifying consumer panel households
        iv. Influencing consumer panel households

Part II.D Location Based Data

A. Some location based research and advertising platforms have first party relationships with those whom they *contact*. However, often location based services are based on data aggregated from many (hundreds of) apps that have requested to know a user's location. App users will likely not know that their location is being shared with aggregators permitting *contact* with many millions of people based on location.

i. The member service delivering a location based *contact* must identify on their website what sources of data are used and provide those targeted with the ability to opt-out of future *contacts*
ii. Since the initial app user would not know why the message was delivered, members should include a tracking function such as adChoices to enable a user to understand from where the survey, ad or other message was delivered making it possible to op-out
iii. As would be implied under the Chain of Trust Principle, Code compliant members would only work with location services that are compliant with all consumer privacy regulations

GLOSSARY

Affiliated Companies: Companies that share the same parent organization or ownership. For example, two companies owned by the same holding company are affiliated companies.

Anonymized Data: Refers to irreversibly severing a data set from the identity of the data contributor in a study or project to prevent any future re-identification, even by the study or project organizers under any condition.

Artificial Intelligence (AI) : In Ad Tech, this refers to algorithms that learns from continued data or human feedback. AI uses may include but not limited to media planning, dynamic creative optimization and developing target segments.

Biometric: Research techniques that use measures such as eye-tracking, galvanic skin response, heart rate, facial coding and other physical measures of response. It may also include neuro research.

Code: This Code is intended to serve as strong guidelines, the adherence of which would support industry self regulation. Membership in the ARF does not require a total adherence to every element of this Code. However the ability to display the Code logo, requires substantial adherence to all relevant elements of this Code.

COPPA: Rule Summary: Chidrens Online Privacy Protectoion Rule - imposes certain requirements on operators of websites, mobile or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

De-identified Data: Also referred to as pseudonymized data, de-identification is the process of severing a data set from the identity of the data contributor, but may include preserving identifying information which can only be re-linked by a trusted party in certain situations.

HIPAA: The Health Insurance Portability and Accountability Act of 1996 is the United States legislation that provides data privacy and security provisions for safeguarding medical information.

Instrument: In this context it refers to the tool used to collect information. More traditionally, it refers to survey questionnaire, focus group guides, diaries and similar devices. Today, it may more broadly refer to electronic or passive means of collecting data such as meters, mobile phones and online behavior.

Interest Data: Generally refers to online behaviors such as search or social which imply an interest in a certain subject.

Must: Implies strong adherence is required to meet the Code. In contrast to “should” for which there are a broader set of exceptions. See should, below.

Neuro: A subset of biometric research that measures memory, attention and emotion through EEGtechnology.

Online Behavioral: Data on web usage, app usage and navigation generally used to classify a cookie, IP addres or device id into advertising targets.

Placebo: A fictitious entity, such as company or product name, used in research.

Should: Implies a broader set of exceptions to a strict code. See must, above.

Syndicated Data: Data which is collected by one or more companies where the same data sets are sold to many purchasing clients.

Targeting: The practice of delivering an ad to a specific person or device, or groups of people or devices, based on known or inferred characteristics of those people or devices.

Appendix 1
Industry Codes and Documents Used in the Compilation of
The ARF's Member Code of Conduct

1. Amazon Privacy Policy
2. Apple Privacy Policy
3. American Association of Advertising Agencies
4. American Association for Public Opinion Research Code of Professional Ethics and Practices
5. ANA and Reed Smith LLP, The General Data Protection Regulation (GDPR): What U.S. Marketers Need to Know
6. ASRC Accountability Program Decisions, Dispositions, Closures, and Guidance
7. Axicom US Products Privacy Policy
8. Axios Media Trends
9. CASRO Code of Standards and Ethics for Market, Opinion, and Social Research
10. Center for Plain Language Privacy-policy analysis
11. comScore Privacy Policy
12. Data & Marketing Association (DMA) Annual Ethics Compliance Report
13. Data & Marketing Association (DMA) Guidelines for Ethical Business Practice
14. Digital Advertising Alliance: Application of Self-Regulatory Principles to the Mobile Environment
15. Digital Advertising Alliance: Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices
16. Digital Advertising Alliance: Self-Regulatory Principles for Multi-Site Data
17. Digital Advertising Alliance: Self-Regulatory Principles for Online Behavioral Advertising
18. ESOMAR Use of Secondary Data in Market, Opinion, and Social Research and Data Analytics
19. eXelate, A Nielsen Company Services Policy
20. Facebook Privacy Policy

21. Federal Trade Commission: Cross-Device Tracking
22. Federal Trade Commission: Marketing Your Mobile App
23. Federal Trade Commission: Privacy & Data Security Update 2018
24. GfK Privacy Policy
25. Global Data Protection Regulation
26. Google Privacy Policy
27. IAB Code of Conduct
28. ICC/ESOMAR International Code
29. INDAIS A Better, Safer Data Exchange
30. Insights Association Code of Standards and Ethics for Market Research and Data Analytics
31. Instagram Privacy Policy
32. IPSOS Neuroscience POV
33. IPSOS Privacy Policy
34. Kantar Cookies and Policies
35. Kantar Media Privacy Statement
36. Lucid Privacy Policy
37. Nature, "Cambridge Analytica controversy must spur researchers to update data ethics"
38. Neustar Privacy Policy
39. Netflix Privacy Policy
40. Nielsen Global Privacy and Data Use Policy
41. NMSBA Code of Ethics
42. Oath Privacy Policy
43. Official Journal of the European Union Regulations
44. Oracle Marketing Cloud & Oracle Data Cloud Privacy Policy

45. Pinterest Privacy Policy Updates

46. Salesforce DMP Privacy

47. Snap Inc. Privacy Policy

48. Spotify Privacy Policy

49. TechCrunch, "Facebook plans crackdown on ad targeting by email without consent "

50. The Advertising Research Foundation Knowledge Center Custom Research Request

51. The Market Research Society (MRS) Code of Conduct

52. The New York Times, "Facebook is Not the Problem. Lax Privacy Rules Are."

53. Twitter Privacy Policy

54. Viant Privacy Policy

55. WARC: The World Media Group guide to GDPR - in plain English

56. WOMMA Code Of Ethics and Standards of Conduct

57. YouTube Privacy Policy