the audience agency

TAA approach to research ethics, data security and GDPR

Ethical Standards

The Audience Agency is committed to upholding ethical standards in all its work. As part of our project setup we review the characteristics of the target research participants alongside the research objectives, particularly where it involves vulnerable or isolated individuals or communities. This approach assesses the most appropriate methodology for data collection, ensure that only data required to assess the project against outcome and impact criteria is collected, all welfare issues are considered and that ethical approval is sought from the relevant overseeing body for the sector involved if necessary.

If required, disclosures and barring checks for individuals delivering projects will be undertaken (if not already in place) and delivery will comply with all relevant safeguarding policies and procedures.

This ethical review process is revisited to ensure full compliance and should any particular issues be raised during a project, a structured process would be instigated to address them.

Equality & Diversity

TAA's core purpose is towards the creation of a more diverse culture and equal society. This is reflected in the diversity of our staff and stakeholders, while this principle also informs our values and commitments.

Alongside our quality assurance and ethical review processes we ensure that the welfare, identity and security of all research participants is respected. Where appropriate methodologies are adapted and revised to enable equitable participation.

GDPR, Quality Assurance and Analysis Processes

The Audience Agency group adheres to strict data terms of use and quality assurance procedures. We comply with our obligations under General Data Protection Regulations (GDPR), and the Privacy & Electronic Communications Regulations (2003). All data is stored on EU-based servers. We are registered with the Information Commissioner's Office with registration ZA009719.

the audience agency

Research respondents' identities are protected, with all data stored securely, reporting anonymised and permissions gained from respondents, carers and guardians for involvement in the evaluation.

We follow standards which ensure data integrity, data checking and internal peer support for delivering findings. The quality assurance process includes:

- **Clearly documented brief and deliverables at the outset of projects, agreed with client.**
- **Where appropriate, the use of standard question sets enabling wider comparison and benchmarking.**
- **Collection of contact details from face to face survey respondents for quality assurance follow up.**
- **All survey data is checked in a number of ways. This includes consideration of partials, speeders, multiple responses. We conduct tests of question completion to check they are being understood and where appropriate we randomise categories in surveys. We have Documented research processes for:**
    - **Data merging and cleaning**
    - **Aggregation of fields**
    - **Use of standard and widely tested graphing templates.**
- **Inclusion of margins of error and base for each question (in report of supporting excel summaries as appropriate).**
- **Adherence to industry-standard 95% confidence and samples to enable 5% margin of error as standard. Required sample sizes to achieve this will be included in proposals.**
- **Stratified sampling and weighting of survey responses, as appropriate (to be agreed with the client in advance).**
- **Review of reporting by consultant, with detailed contextual understanding, to test the findings through interpretation and to ensure fit to the brief (i.e. delivery of different aspects of the project by relevant specialists).**

Where we sub-contract work, we ensure that equivalent standards are met by our suppliers.

the audience agency

Security and Confidentiality

All our systems are monitored, and protected by anti-virus software, and are protected by our own and Microsoft's systems. All our data, systems and applications are protected by multi-factor authentication to reduce any risk of sign in violation, or password loss. We have alerts programmed to prevent unauthorised data removal, and data loss processed supported by our cyber insurance coverage. We have disaster recovery processes in place to be followed as required.

TAA do not send or receive personal/confidential respondent data by email. Instead a secure data files sent to and from TAA containing personal information should be sent via our MailBigFile SFTP service.

Both our physical offices are secured, with multiple-locking facilities, managed by limited and monitored keyholders. Both offices are also covered by remotely monitored alarm systems. We have full insurance coverage for property, people and activities.