



Qualitative Research Recruitment - Legal Requirements and Best Practice: Guidance for Recruiters

Introduction

This Guideline sets out the legal requirements and best practice for qualitative recruitment to assist practitioners in understanding their obligations. This document supports the MRS Recruiter Accreditation Scheme (RAS), which has been developed to raise the profile and status of Recruiters by devising a training and accreditation scheme that recognises the knowledge, skills and competence of professional Recruiters.

This best practice Guideline complements the MRS Guidelines for MRS Company Partners: Qualitative Recruitment which set out the legal requirements, process standards and MRS Code rules that relate to the practice of qualitative recruitment, which aims to support MRS Company Partners to better understand their corporate obligations when buying and/or undertaking recruitment.

The purpose of the best practice documents, and the Recruiter Accreditation Scheme, is to improve understanding and adherence with all the relevant legal and ethical requirements.

A compliance framework for the RAS is being developed and will be issued for consultation with recruiters later this year.

It should be noted the best practices covered within this document are issues that are generally considered to be most relevant to recruitment practices. However, there are specific rules for certain sectors and disciplines, such as the BHBIA and EphMRA standards for health research recruitment, which should also be adhered to in addition to this guidance.

Key Definitions

Controller: Sometimes called a “Data Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Protection Act 2018: The Data Protection Act 2018 is an Act of Parliament which defines UK law on the processing of data on identifiable living people. The Data Protection Act controls how personal information is used by organisations, businesses or the government.

Data Subject: are identified or identifiable living individuals to whom the personal data that is held relates.

Joint Controller: is where two or more controllers jointly determine the purposes and means of the processing of the same personal data.

Personal data: means data that is wholly or partly by automated means; or the processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system. Personal data only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information.

Processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor: Sometimes called a “Data Processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Recruiter: means a person or organisation which sources and recruits participants for in market and social research activities. Recruiters are used mainly for qualitative research e.g. recruitment of participants for focus groups, depth interviews, ethnographic research, UX testing, etc.

Sensitive Personal Data - Special category data (sometimes called sensitive data as it needs more protection when it is being collected) means personal data about an individual's (a 'data subject'):

race
ethnic origin
politics
religion
trade union membership
genetics
biometrics
health
sex life
sexual orientation

In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. In addition, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, and largely the same conditions apply to this data as with special category data.

Third party: means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Key Legal and Ethical Requirements

Data Protection Fee

1. Recruiters may determine the purposes for which personal data they collect are to be processed to meet their clients' requirements. Consequently, Recruiters are Data Controllers and must pay an annual data protection fee their data activities, which is administered and regulated by the Information Commissioner's Office.

Contracts

2. The rights and responsibilities of Recruiters, their clients and any sub-contractors used must be governed by written contracts.
3. Contracts, in addition to commercial terms (fees, payment dates and so on) must include all relevant research and data details, for example:
 - The purpose of the data processing
 - The subject matter
 - The dates (from and to) of the data processing
 - What the processing activities are e.g. recruitment screening, sending participant profiles, etc
 - Types of personal data being collected e.g. name, email, addresses, financial information
 - Any special categories of personal data e.g. ethnicity, health data, etc.
 - Categories of data subject e.g. employees, subscribers
 - Any data transfer requests e.g. the method for sending participant profiles
 - Any end of contract requirements e.g. returning client supplied samples

Note: a contract can be an exchange of emails or any other written document setting out the agreed terms for a project. There must always be evidence that a contract has been entered into and accepted.

4. Recruiters must provide regular updates on recruitment progress (as specified within contracts / statements of work), particularly on any problems or questions that arise. Recruiters should raise any questions or queries relating to projects as soon as possible with clients, to avoid contractual problems later.
5. General advice on contracts is available via the RAS GDPR training module.

Consent

6. Data collected by Recruiters from research participants must be collected with informed consent i.e. participants must be informed fully about the purpose, methods and intended possible uses of their data, what their participation in the research entails and what consequences apply. This information would normally be relayed via recruitment documentation including invitations, screeners, etc.

Informed consent requires the following information to be provided:

- a) the name of the organisation(s) or individual responsible for data collection;
 - b) the general subject of the data collection;
 - c) the purpose of the data collection;
 - d) the type of data collected, particularly special category and/or criminal convictions data;
 - e) the right to withdraw at any time;
 - f) whether the data collection is to be recorded and/or observed;
 - g) who is likely to have access to live or recorded information;
 - h) the likely length in minutes of the data collection;
 - i) any costs likely to be incurred by a participant;
 - j) the use of automated decision making (if used);
 - k) transfer of data to a third country;
 - l) retention periods or criteria used to determine retention periods;
 - m) the right to complain
 - n) an assurance that the activity is being conducted in accordance with the MRS Code of Conduct and the Data Protection Act 2018 and/or local data protection legislation for non-UK activities.
7. Recruiters must adhere to informed consent requirements for any supplementary activities undertaken, such as participants being added to recruitment databases.

Note: Recruiters can only add participant details to recruitment databases if this is allowable within the contracted terms of any project being undertaken. For example recruitment using end-client supplied customer data may explicitly restrict such activities.

Recruitment

8. There are a variety of methods that can be used to effectively recruit participants for research projects. These will vary depending on the type of research and the mix of participants that clients are seeking. The most common approaches are:

- *Free find:* Recruiters use their own methods to find participants whether that be in store, on street, desk research or via their network or database.
- *Client list:* Recruiters use end client provided customer samples to recruit participants e.g. a high street bank may give a list of their current account customers to be invited and screened for a focus group.
- *Social media:* Recruiters use social media platforms e.g. Facebook, LinkedIn, etc. to recruit participants who use social media. Social media is suitable for recruiting specified segments of the population and niche audiences, e.g. recruiting upcoming music artists who do not have a huge fan base – targeting fan pages on Facebook would allow Recruiters to check and see who exactly “likes” the relevant music.

The key principle when using social media is to ensure that detailed specifications are not included as part of the recruitment activity. This avoids the temptation for potential participants to flex their profiles to meet recruitment specifications. For more guidance see the RAS New and Emerging Recruitment Techniques module.

Note: particular care should be taken to establish the confidential nature of the client or project being undertaken, and not inadvertently disclose such information during the recruitment process. For example, publishing recruitment details online about a group discussion that discloses client business sensitive information.

- *Cold calling/ cold emailing:* Recruiters use cold calling and/or cold emailing usually where there is no sample list provided by a client and the recruitment requires targeting certain audiences, e.g. business to business recruitment where lists of relevant companies can be built using online search and potential participants identified and targeted via email or telephone contact.

Recruiters using the cold calling/emailing method need to be familiar with the restrictions of unsolicited email as defined by the Privacy & Electronic Communications Regulations. Advice on the Regulations are available on the MRS website.

- *Street recruitment:* Recruiters use street recruitment mainly when it suits the nature of a research project e.g. recruiting participants that use a certain bus stop, or shop at specific media outlets.
- *Online website recruitment:* Recruiters use a variety of online recruitment techniques, including pop-ups and banners, which can be useful when websites have visitors which are likely to meet identified recruitment criteria.

The AQR Recruiter training developed for this Scheme details best practice approaches for each of the above techniques. The training can be accessed via the RAS website: <https://ras.mrs.org.uk>

9. Once participants are recruited, Recruiters must relay all key information and ensure that this is followed up in a written communication (email or letter). Information which must be communicated includes:

- The name of the organisation or individual responsible for the data collection including relevant contact details
- The general subject to be covered, specifying if any sensitive topics are likely to be discussed e.g. sexual health
- The purpose of a discussion (market research) and the type of discussion (e.g. group, depth, paired depth, etc.)
- The date, time, duration and venue (with full address and map where necessary)
- Whether an incentive is to be paid, when it will be paid, how incentives will be administered and by whom, and any conditions for the payment of incentives e.g. completion of pre-tasks.
- Whether any observation and/or recording is to take place and how any recorded data will be used, including details of those that will have access to live and/or recorded data.
- Whether any costs are likely to be incurred by participants.
- Any additional requirements (such as a pre-task, telephone interview, etc.)
- Any possible consequences because of participating (e.g. re-contact for subsequent research) and obtain consent if this is to occur.
- An assurance that the activity is being conducted in accordance with the MRS Code of Conduct.

10. It is the recruiter's responsibility to ensure:

- The terms of any recruitment contract have been met
- All participants are recruited to specification and any changes to specification have been agreed with clients beforehand
- Profiles for participants are supplied within agreed time frames and format/s
- Participants arrive at the right place at the right time
- All participants understand what is expected of them

It is generally not the recruiter's responsibility to ensure:

- Venues are booked and refreshments are ordered
- Administer incentives

Quality Control

11. Recruiters must undertake some quality control during the recruitment process as this will be important to the overall success of research projects. Several steps can be put in place by Recruiters to ensure the recruitment of quality participants, which meet any required specifications:

- *Monitor repeat attendance:* internal systems need to be used to check participants have not undertaken similar studies before.

Note: It is accepted that there are limits to how much Recruiters can track repeat attendance via other Recruiters. The key issue is that Recruiters ensure that fresh participants are used for all of their studies unless past participation is not considered a barrier for participation (e.g. for some healthcare studies).

- *Meet the brief:* the screening process must be followed to ensure that participants match any research requirements; and if during this stage any participants are found to not fit a quota, for whatever reason, the participants must be eliminated from taking part.

Pre-check calls are an essential part of the recruitment process, usually undertaken by field suppliers, to ensure that specifications are met. It is essential therefore that Recruiters are confident that participants recruited meet the agreed specifications.

- *Checking Identities:* Recruiters must agree with research and/or field suppliers how participants' identities will be checked, ensuring this is relayed to participants at the recruitment stage.

Methods of confirming identities are generally a matter for field and research service providers. Confirming identity from participant's ID documentation is the best approach.

Note: There are a variety of methods for confirming identities. The evidence used must be credible third-party evidence such as passport, drivers' licence, and other photo IDs (e.g. Validate UK and other such schemes). In rare cases it may not be appropriate to check ID documentation, if this is the case detailed reasoning must be documented including other methods used to confirm participant identities.

- *Confirming recruitment criteria:* Confirmation of participants matching recruitment criteria is generally a matter for field and research service providers. Confirming recruitment criteria can involve the use of self-completion questionnaires, formal questioning of participants or can be based on the judgement of moderators (the latter is likely to be an integral part of moderating although its subjective nature should be considered in terms of robustness for quality control purposes).
- *Follow-up:* if something has gone wrong, all relevant parties including Recruiters must undertake follow-up action to reduce the likelihood of future repeat problems.

More details about the role and responsibilities of recruiters is available via the RAS training modules: <https://ras.mrs.org.uk>

Data Security, Retention and Destruction

12. All data collected and retained for research recruitment purposes, must be kept securely by Recruiters, without any unauthorised access or use.
13. Recruiters must take reasonable steps to ensure that all hard copy and electronic files containing personal data are held, transferred and processed securely in accordance with relevant client data security policies and/or contractual obligations.
14. Recruiters must take reasonable steps to ensure that the data retention and data destruction is adequate for the confidentiality of any data being retained and/or destroyed. This would include for example:
 - Adhering to data retention policies e.g. retaining primary recruitment records for 3 months after a project is completed and then confidentially destroying them, unless client retention periods state otherwise.
 - Selecting appropriate data destruction approaches as appropriate for the type of records (e.g. paper, digital, recorded) and the sensitivity of the data being destroyed (e.g. health and financial records would require higher levels of safeguards).

More details regarding data protection, security, retention and destruction are available via the RAS GDPR training module.