

Guidance – Online interviews and focus groups

Related Policy: [Data Protection Policy](#); [Guidance on Research in the Digital Space](#); [Research Data Management Policy](#): Things to Consider.

Approved by:

Effective Date: 17 October 2025

Supersedes: N/A

Next Review: 1 October 2026

1. Introduction

- 1.1 Please follow this guidance if you are, or planning to, use video conferencing platforms such as Teams or Zoom to conduct interviews and focus groups as part of your research project.
- 1.2 Teams is the University's default platform and should be used to conduct interviews or focus groups. If you would like to use another platform, the rationale for this must be recorded and approved by the Principal Investigator in advance.ⁱ

2. Is online appropriate?

- 2.1 Conducting interviews and focus groups via Teams offers convenience to both the research participant and research team, however, its use may not be suitable in all circumstances.
- 2.2 It should not be assumed that all participants will have the required access in terms of devices, data, and privacy.
- 2.3 It may also be difficult for participants to find a space to be alone, quiet, and not overheard. This is of particular concern when the interview/focus group will involve the discussion of sensitive subjects, e.g. sexual health, traumatic events, drug use or criminality due to the potential for distress and the lack of end-to-end encryption as standard on Teams. It is vital that the circumstances under which video conferencing such as Teams when in use between interviewees and interviewers is safe, secure and silent, with no risk of disclosure of content, or the appearance of additional/accidental persons (in the background) who are not informed participants in the research.
- 2.4 End-to-end encryption may be made available on Teams on application. End-to-end encryption is appropriate for research conducted using MS Teams that has high sensitivity. Digital and Information Services should be contacted to discuss if this possible.
- 2.5 You should outline the appropriate steps you will take to manage the safety, security and integrity of your research, as detailed in a [Data Management Plan](#). You can gather further

advice from the [Research Data Librarian](#).

3. Using Teams for online interviews

- 3.1 Teams can be downloaded onto computers and mobile devices, or it can be accessed via any web browser.
- 3.2 To use Teams to conduct an online interview you will need to create a meeting in your University Outlook calendar and invite participants to this using their email addresses. You can find instructions for how to do this on the Microsoft webpages [here](#).
- 3.3 Give your meeting an appropriate name and avoid using any personal data in the meeting details.
- 3.4 Email addresses provided to facilitate online interviews must be held securely and separately to the research data. How email addresses are managed, including how long they will be kept, should be detailed in the research protocol/[Data Management Plan](#). If participants are to be anonymous, it is vital that the meeting is set as “private.” This ensure that all those who have visibility of the Outlook calendar of the researcher organising the interview or focus group cannot see the names of the participants taking part. Information about making a Teams meeting/appointment private can be found [here](#).
- 3.5 Participants must be signposted to the [University’s research participants’ privacy notice](#) and to [Teams Privacy Policy](#) so they are fully informed as to what data is collected and what it is used for.3.5 When using Teams, you must not use your personal account/email from which to set up an online interview or focus group.
- 3.6 Avoid using public Wi-Fi networks. Instead, it is recommended that you use secure, private networks to prevent unauthorised access. In terms of access control, limit access to the online interviews and recordings to authorised persons only. Use strong passwords and enable waiting rooms or similar features to control who joins the meeting.
- 3.7 When using Teams, consider the location of the participant(s) and confirm their ability to participate while being in a private location.
- 3.8 You could consider if an audio-only option is advised for the online interview. This may ensure greater security if there were a breach or hack.
- 3.9 If video recording of the interview is needed, this needs to be stated in the Participant Information Sheet and clear, informed consent needs to be secured.

4. Settings in Teams

- 4.1 Attend to security settings in Teams. It is advisable that only organisers and co-organisers can bypass the lobby. This means that the organiser would have to approve everyone in attendance of the interview. This increases security and ensures that participants who attend online have been approved.
- 4.2 For audio and video settings, the [organiser of the interview can toggle camera and/or audio of for attendees](#). If you plan to video record the interview, but you do not wish for the

participants to be visible, you should not enable camera for attendees in the toggle setting under audio and video setting options.

- 4.3 It is important to be aware that an attendance report can be generated in Teams. If you do not wish for this to be a feature, ensure the toggle is switched off.
- 4.4 It is advisable to set the meeting as private.
- 4.5 It may also be advised under response options to not allow forwarding. This would ensure that participants aren't permitted to forward on the meeting request to anyone else. This ensure that the meeting only has designated persons in attendance.

5. Using Teams for focus groups

- 5.1 As with setting up an online interview, to set up focus group you will need to create a meeting within your University Outlook calendar. Ensure that the meeting is set as private.
- 5.2 Given the collaborative nature of Teams, participants are likely to be able to see the names, initials, profile pictures, and possibly faces and/or voices, of other participants in the group. Participants should be made fully aware of this the Participant Information Sheet.
- 5.3 You can minimise the amount of personal information accessible advising participants if they join as 'guests' when asked to provide a name they can provide a pseudonym.
- 5.4 However, if participants join via their own Teams account (either a personal or work account), they may be unable to change their displayed name. Again, this should be made clear in participant information.
- 5.5 The protocol/Data Management Plan should detail how email addresses provided to facilitate a focus group will be managed (please see 3.3, 3.4).
- 5.6 Privacy notices must be signposted to participants (please see 3.5).

6. Recording and transcription

- 6.1 If you intend to record the interview/focus group you must advise participants in advance. You should also advise participants that they may not record the meeting(s). Please familiarise yourself with the settings in Microsoft Teams regarding the options for [who can record and transcribe an online meeting](#).
- 6.2 Recordings from Teams (or Dictaphone) should be immediately downloaded and saved to secure storage with backup. It is advised also that the recording/s are saved in an encrypted folder in your secure storage. Any extant copies of the recording should then be removed from Teams and/or Dictaphone.
- 6.3 Teams does provide a transcription function; however, the transcription may not be completely accurate. If using the transcription function, or any other transcription software or service, participants must be advised in advance.

- 6.4 If product used leverages generative AI, you must be aware as to how the information is shared and used to develop products and services, including training AI models. This information must be provided to participants in advance of any data processing.
- 6.5 Researchers should also consider and have in place the appropriate consent to facilitate the use of digital/AI transcription. Researchers should also consider the sensitivities of their work and whether it is appropriate for that data to be transferred to an external party.
- 6.6 Other transcription software/services may require a data processing agreement to be put in place – please contact the [Information Compliance Unit](#) to facilitate this.
- 6.7 On completion of transcription, and only after the transcription has been verified, all recordings should be deleted, unless it is necessary to retain e.g. funder requirement.

7. Sharing transcripts

- 7.1. If you intend to share voice and/or video recording of participants via online interviews and/or focus groups, it is essential that you have informed consent to share this content. Selecting the appropriate repository and access controls for this content are vital. To this end, it will be necessary for you to discuss with the [Research Data Librarian](#).
- 7.2 If you intend to share transcripts of your interviews or focus group in a public-facing repository, you will need consent from your participants for this. It is advised to share in [Queen's data repository](#) or [UK Data Service](#). Please consult the [SOP Informed Consent for Research](#). You should have also planned for your [data sharing](#) options in your [data management plan](#). Please contact the Research Data Librarian for further information.

8. Further guidance

8.1 [See Research in the Digital Space: Things to consider](#)

- 8.2 This guidance is not exhaustive. If you require further advice, please see useful contacts below:

Information Compliance Unit – info.compliance@qub.ac.uk

Research Governance, Ethics and Integrity – researchgovernance@qub.ac.uk

Research Data Management Library Services – rdm@qub.ac.uk

ⁱ [Queen's University Belfast utilises Microsoft 365](#), a range of cloud-based services, including Teams, OneDrive, Word, Excel and PowerPoint. Microsoft Teams is the usual default for conducting interviews and focus groups online across the University. Other platforms may have associated risks. Zoom, for example, has, in the past, been prone to hacks e.g. Zoom bombing.