Guidance for research online

Prepared by the Research Ethics and Governance Team at the University of Exeter in response to the COVID -19 restrictions on face to face research activity. This will be updated as further information becomes available and is subject to change, please ensure you access the latest version (currently v1.0, Apr 2020).

When conducting research with participants remotely, additional care needs to be taken to ensure that the participants are not exposed to the following risks:

- Breach of privacy and confidentiality
- Identification and re-identification of participants who have been offered anonymity or pseudonymity (linked-anonymisation)
- Loss of jurisdictional legal rights through transfer of personal data outside the EEA, EU and United Kingdom
- Excessive accumulation of personal data that is not necessary for the aims of research
- Interception and surveillance of communications that would not have been possible in a face-to-face setting
- Loss of certainty about withdrawal and destruction of data.

Given these risks, consideration should be made before determining whether remote interviews or surveys are safe for participants.

- What are the additional risks to participants and how can they be mitigated?
- Could the research be conducted at a different time by meeting face to face?
- Does the research depend on establishing a rapport with the participant that may be inhibited or unobtainable by remote means?
- Will the preferred method of remote data collection lead to excessive collection of data that is not necessary to the research? Examples – would a telephone call suffice rather than a recorded video conference? Does the survey contain questions not directly relevant to the research?
- How will the participant be informed of the research methods and provide consent?
- How can the participant maintain anonymity if required/preferred?
- How can the participant withdraw all data from the study so that the researcher is in full compliance with such requests, or at what point will data be disposed so that it becomes genuinely impossible to identify the participant?
- Is the participant or the research topic of interest to 'motivated intruders' who may use sophisticated methods including forced entry, mass surveillance and/or keyword surveillance to intercept the communications?

These are just examples; other circumstances may throw up ethical issues that a Research Ethics Committee or reviewer may consider to be a risk to participants or to the researcher.

TELEPHONE BASED RESEARCH

Whilst being simpler and less data heavy, consideration should be given to the management of data and privacy of both researcher and participant.

Disclosure of personal numbers may be a risk to both participant and researcher. Researchers should not use personal numbers to make calls but instead use work lines or dedicated mobile SIMs for use in making calls.

Recording of calls should only take place with the prior informed consent of the participant who may request the recording stop at any time and request the recording be deleted.

Mobile recording apps that transfer data outside GDPR jurisdictions should not be used. Preferably, recordings should be made using encrypted recording devices not connected to the internet; with the recording then uploaded to University OneDrive or secure network drives using VPN when off campus.

Most telephones have native network conference call capabilities and do not need the additional services such as 'PowWowNow'; which may transfer data outside GDPR jurisdictions. If such services are to be used, privacy policies should be investigated in advance to ensure the risks specified above are addressed.

Hybrid solutions are possible; for instance using Teams or Skype for Business dial-in access to conferencing which may provide scope for telephone participation.

ONLINE VIDEO CHAT AND CONFERENCING

The University usually requires the use of Microsoft Teams or Skype for Business for online discussion and collaboration with research participants.

Both applications are able, using email and publicly posted web link invitation, to include guests in online discussions and conferences. When used with a University account, meetings may be recorded, though participants should be informed and consent in advance to such recording.

Guides

Microsoft Teams for Students **Microsoft Teams for Staff**

Skype for Business

When used with a University account, both Skype for Business and Microsoft Teams are compliant with University of Exeter information Governance policies and GDPR.

Other applications (which may be preferred by individual users) will probably not be compliant. Use may cause a degree of risk to your participants as there may be data leakage. For example; one popular competitor to Teams was found to be collecting and reselling data from calls to advertisers to target personal advertising at participants. Other applications may be more vulnerable to motivated intruders with state surveillance capabilities using brute force methods to gain access to discussions.

Use of other applications:

Before deciding that you'd like to use another video conferencing app, what exactly is it that you would *not* be able to do in either Skype for Business or Microsoft Teams that you could do in other applications?

You will need to ensure that your understanding of the features for either package is current; then be sure that use would prohibit your desired method of research; and that method is crucial to the outcomes of your research.

If you can achieve your aims by using Skype for Business or Microsoft Teams rather than another app, then for the safety of your participants and security of your data you must do so.

One argument against using Teams or Skype for Business may simply be convenience or familiarity of participants with another application.

When this arises, participants should have first been offered and rejected the use of Skype for Business and/or Teams then requested an alternative solution. Researchers should inform participants regarding the potential risks to their data arising through the terms of use and privacy policy of the application and ensure that they consent to participate knowing these risks.

MOBILE PHONE APPLICATIONS INCLUDING 'CHAT' APPLICATIONS AND SOCIAL MEDIA

Given the considerations outlined on Page 1 use of mobile apps cannot be usually be recommended, but inevitably will be proposed, possibly as a means of recruiting participants. Caution should be taken when proposing or reviewing the use of mobile applications. Researchers should clarify what interactions will take place, particularly using social media messaging services.

- Several mobile applications do make a virtue of being very secure. This includes WhatsApp, Apple Messenger and FaceTime, Telegram. These may be considered as research tools and present a risk roughly equivalent to using Skype or Teams
- Others such as Facebook Messenger are *not* secure. Insecure applications that harvest data and have loose privacy setting should preferably not be used
- When selecting an application for use in communicating with participants through messaging or social media, the purpose of such communication should be justified. Use of applications should be contingent upon informed consent by participants
- When using applications that are regularly intercepted and moderated by authoritarian regimes, the design of the research should give particular consideration to asymmetrical risks posed to participants from regime surveillance and appropriate steps taken to ensure participation does not expose the participant to harm from the regime.

ONLINE SURVEYS

When using on-line surveys, researchers should ensure that before their survey starts, there is an information sheet and consent form as the first page of the online survey; this ensures that participants may make an informed judgment about whether they wish to participate in the survey.

Consent should be obtained from the participants by providing the consent document and requiring participants to click a button or type out a statement of agreement indicating consent to participation before proceeding. Researchers should also include an option that will allow the respondent to withdraw from the survey at any point.

UoE Template Participant Information Sheets and Consent Forms are available here and can be used (with appropriate adaptation) by researchers for online purposes. The UoE Privacy Notice for Research is available here and should also be provided to the participant.

If you have any queries regarding on-line surveys please contact the Research Ethics and Governance team

More external information and guidance on conducting surveys is available in the resources listed below.

ONLINE SURVEY TOOLS

Researchers must ensure that any online survey tool used states that personal data is held/hosted on servers within the UK, EU or European Economic Area (EEA) to comply with GDPR regulations and protect jurisdictional legal rights; that may be lost if data is transferred to a non GDPR jurisdiction.

Any survey tool transferring data outside a GDPR based data jurisdiction (such as the United States) does not provide participants with rights enforceable through GDPR and therefore should not be used. EU data adequacy provisions as exist with Switzerland and the United States do not afford sufficient protection to participants.

The University subscribes to the following survey tools;

Survey tool	Available to	
	Staff	Student
Microsoft Forms – using your University Office 365 account Microsoft forms is a suitable tool for online surveys and forms part of the University Microsoft Office 365 subscription licence suite, which is available to both staff and students using their University single sign on to Office 365. More information is available here; **http://www.exeter.ac.uk/it/howdoi/office365desktop/**	✓	✓
JISC Online Survey The People Development team subscribes to the JISC Online survey tool (formerly Bristol Online Survey). Registration is available to staff only (although PGR students may be able to access on request) and information on how to register is available here: **http://www.exeter.ac.uk/staff/development/about/onlinesurvey/**	✓	x *(PGR students may be able to access on request)*
Qualtrics Some colleges subscribe to Qualtrics the main subscriptions are for SSIS, CLES and UEBS which are administered by IT. These subscriptions are dedicated to specific colleges or projects and the licensing conditions prevent them being used by others in the university. Please check with your college IT partner to see if there is a subscription for your college and contact IT helpdesk/SID for more information and access. **https://www.qualtrics.com/uk**	*Depends on college subscription*	*Depends on college subscription*
Lime Survey The University has a couple of self-hosted Lime Survey software installations **https://www.limesurvey.org/** which are administered by IT. Please contact IT helpdesk /SID for more information and access.	✓	✓

For ease of access we recommend you use Microsoft Forms via the University Office 365 sign-in; there is no 'gatekeeper' which means you can start without any delay.

Doctoral students are reminded that online survey expenses may be met out of the Doctoral Study allowance. Contact the Doctoral College for further information. If you require a more complex survey with advanced features, or you are recruiting participants via Prolific.co or MTurk; then you may need to use a survey tool like Qualtrics.

BUILDING TRUST WITH PARTICIPANTS

Consider methods to ensure that your participant feels confident and safe during the interview.

- Use research methods that are trusted and will provide participants with confidence
- Ensure participants have full information that is comprehensible using appropriate language
- Reconfirm consent whenever an interview commences or re-commences
- When using telephony, consider providing a pre-arranged 'code word' prior to the call/interview that will be used to verify the identity of the caller
- Always be clear whether or not the conversation is being recorded and remind participants of this at the start of every conversation. If a conversation is being recorded, information about how (and when) consent to recordings may be withdrawn and the data deleted must be provided and informed consent is needed. Resources such as the SHARE checklist **UK Government SHARE Checklist** or the Information Commissioner's Office can help participants (and researchers) to understand why some measures and safeguards might be necessary.

Resource links:

Academic research: integrating security and privacy

Association of Internet Researchers

British Psychological Society Ethics Guidelines for Internet-mediated Research

ESRC Guidance on internet mediated research

Health Research Authority

Information Commissioners Office: Community groups and COVID-19: what you need to know about data protection

JISC: Staying secure on social media: a quick guide for academics

NHS Information Governance Advice

The British Psychological Society

UK Government SHARE Checklist

V 1.0 April 2020