Guidance for undertaking research using phone, email and video-conferencing software

1. Introduction

1.1 This guidance is for research with adult participants (over the age 18yrs). It is only a guide and it is essential that you take responsibility for checking the terms and conditions of any online service or software you decide to use. It does not provide a complete review of all video-conferencing systems.

1.2 For research with children under the age of 18yrs, you will need to consider who owns the contract for the device being used, e.g., phone, and the internet service provider (ISP) that they connect with, as under 18yrs olds will not have the legal contract for phones or ISP. Therefore, you will need to gain consent from the parent/carer/adult to use this medium for research.

1.3 It is important to bear in mind that your research will be classed into the following categories namely: (i) minimal risk and (ii) More than minimal risk and (iii) High risk.

Minimal risk projects DO NOT include:

- the collection of any type of personal data;
- focus groups;
- experiments/observation studies
- use of medical devices;
- internet use: i.e. data collection from social media / apps;
- use of mobile devices such as drones;
- children and vulnerable groups (e.g. anyone under 18 years old, adults with cognitive impairment etc)
- sensitive topics (anything deeply personal and distressing, taboo, intrusive, stigmatising, sexual in nature, illegal and potentially dangerous, harmful to national security etc)
- programs / systems / mobile devices / drones: use or development with potential to collect/examine personal/sensitive data (e.g., stored on phones, sat navs, smart TVs etc)

Projects that include the above are classified as “More than Minimal Risk” or “High Risk” and require greater scrutiny for a variety of reasons including: to ensure compliance with legal obligations and to safeguard/protect researchers and participants.

2. **Interviews at a distance**

2.1 If you are conducting interviews over the phone or using video-conference software (e.g. Skype, Whatsapp etc) and NOT recording the interviews (e.g., sound, voice, video, images, name, email address etc) then this may be **MINIMAL RISK** research depending on the subject of the interviews (no sensitive topics) and your participants (i.e., not vulnerable adults and not under the age of 18yrs etc). You must not collect research data and any personal data at the same time.

Informed consent must be obtained from each research participant before any research activity. Before you begin your interview you can obtain informed consent in two ways.

(i) Use of an online CONSENT FORM using Qualtrics. The consent form consists of participant information and a consent statement.

(ii) If the first option is not possible then complete the Participant Information and Consent Sheet (PICS) and send it to each participant (interviewee) via email when you invite them to participate in the interview.

See MyLearning Middlesex Online Research Ethics area at http://mdx.mrooms.net/course/view.php?id=12277 (Log in required) for our guidance on using MU Participant Information and Consent Templates and use of Qualtrics to create an online CONSENT FORM. See Section 4 (Templates – Consent Forms) and Section 7 (QUALTRICS and Conducting Online Research).

1.5 If **you are recording interviews** over the phone or recording video-conference interviews you are collecting personal data. This means you are undertaking MORE THAN MINIMAL RISK research and you will need to provide participants with information on data protection via the University's privacy policy.

Before you begin your interview, you can obtain informed consent in two ways:

(i) Use of an online CONSENT FORM using Qualtrics. The consent form consists of participant information and a consent statement. For MORE THAN MINIMAL RISK projects the participant will have to provide his/her name and email address, and will also be directed to the University's Privacy Policy.

(ii) If the first option is not possible then you need two documents (a) Complete the Participant Information Sheet (PIS) and send it to the participant with (b) the Signed Consent Form via email when you invite them to participate in the interview. Also ask the participant to return the Signed Consent Form to you via email. The form can be signed with a typed name.

See MyLearning Middlesex Online Research Ethics area at http://mdx.mrooms.net/course/view.php?id=12277 (Log in required) for our guidance on using MU Participant Information and Consent Templates and use of Qualtrics to create an online CONSENT FORM. See Section 4 (Templates – Consent Forms) and Section 7 (Online Research).

2. Email/Social Messaging Software

2.1 To make contact with participants it is likely you will need to use email or a form of social media or messaging app to send on a link to a Qualtrics survey. For this to be classed as MINIMAL RISK research you must ensure sure that your Qualtrics survey does not collect any personal data, and that Qualtrics is set to collect data anonymously (see the *Qualtrics Online Survey Guide* on MyLearning).

2.2 Email is not a secure means of communication or for sending documents and should not be used for research which includes sensitive topics (anything deeply personal and distressing, taboo, intrusive, stigmatising, sexual in nature, illegal and potentially dangerous, harmful to national security etc) and/or personal data being collected from participants – unless information is sent in password protected documents and the password is shared in a separate communication. This is because an email travels from the sender's mailbox across multiple networks and servers which may be unsecured, before it arrives at the recipient's mailbox. At each point on its journey, an email is exposed to hackers who can break into unsecured networks and read emails and attachments that are not encrypted. You may wish to consider the following secure email providers:

i) Frama Rmail – simple to use and keeps data secure in transit, it is also tracked and offer e-sign and large documents.
ii) Protonmail – free encrypted email – and ask that your recipient downloads the application too.

3. Video-conference software

With the outbreak of COVID-19 and social distancing requirements and restrictions on movement, video-conferencing has become an essential tool for communication. It is essential that researchers check the terms and conditions of video-conference software before use.

3.1 Skype-C (free Skype-C for Consumers)

Skype has been owned by Microsoft since 2011. See https://www.theregister.co.uk/2017/08/01/skype_for_business/ Note that:

"For existing Skype users, it offered to "upgrade" your Skype name to a Microsoft account by simply adding your email address. But not everybody did. Now, new users of the consumer platform must create or use a Microsoft account.

The Microsoft privacy policy is found here: https://privacy.microsoft.com/en-gb/privacystatement
Essentially, Skype lacks privacy. Microsoft collects, uses and shares your personal data.

"For example, we manually review short snippets of a small sampling of voice data we have taken steps to de-identify to improve our speech services, such as recognition and translation."

See also: https://www.comparitech.com/blog/information-security/is-skype-safe-and-secure-what-are-the-alternatives/ (extract below)

"While Skype-to-Skype calls are encrypted, if you use Skype to call mobile phones or landlines (which many people do in order to take advantage of much lower rates, especially to overseas numbers) the part of your call that takes place over the ordinary phone network (PSTN) is not encrypted. For example, in the case of group calls involving two users on Skype-to-Skype and one user on PSTN, then the PSTN part is not encrypted, but the Skype-to-Skype portion is.

Skype Records Your History

By default Skype will record details about all calls (though not the calls themselves) and store them in a "History" file which resides on the user's device. While this in and of itself is not a problem, if the security of your computer, smartphone or tablet is compromised then the attackers will be able to access its contents."

Also, with Skype, you won't know if the other person is recording the session.

3.2 Skype for Business Online is part of the Office 365 service. Details can be found here: https://docs.microsoft.com/en-us/skypeforbusiness/optimizing-your-network/security-guide-for-skype-for-business-online. This software allows communication with Skype-C users, but this may not be straightforward: See https://www.theregister.co.uk/2017/08/01/skype_for_business/

"Skype for Business is inconsistent in how it handles non-upgraded, standalone Skype accounts. The PC client does let you add people with only a Skype name, if you choose "Add a contact not in my organization" and search the Skype directory. You can chat with them and see their presence indicator. Access your Skype for Business contacts via Office 365 in your browser (finding the Skype icon above Mail or People) and the directory search will find new contacts by their Microsoft account address, but never by their Skype name. Same limitation with the Skype for Business for Mac client, which has no luck finding old Skype names."

Also, you should limit the number of Skype-C contacts you add and be aware of the Skype for Business privacy relationships. It is essential to read this clause:

"Note: By default all external contacts, either personal or federated, will be assigned the External Contacts privacy relationship, which will share your name, title, email address, company, and picture. These contacts will not be able to view your Presence Note. Assigning external contacts to other privacy relationships, for example Work Group, Friends and Family, and so on, will allow them to see your Presence Note and could inadvertently share information that should not be disclosed to them."

If you need to communicate with a Skype-C user, make sure that they incorporate certain privacy settings that will secure their account.

3.3 Zoom
See https://protonmail.com/blog/zoom-privacy-issues/
According to the company's privacy policy, Zoom collects reams of data on you, including your **name, physical address, email address, phone number, job title, employer.** Even if you don't make an

account with Zoom, it will collect and keep data on **what type of device you are using, and your IP address**. It also collects information from your Facebook profile (if you use Facebook to sign in) and any "information you upload, provide, or create while using the service."

Some of this data you enter yourself when you are signing in (for example, to join a call online, you must give your email) but much of it is collected automatically by the Zoom app.

In its privacy policy, under the entry "Does Zoom sell Personal Data?" the policy says, "Depends what you mean by 'sell.'" To summarize Zoom's policy, they say they don't sell personal data for money to third parties, but **it does share personal data with third parties for those companies' "business purposes."** And that may include passing your personal information to Google.

In 2020, after the outbreak of the Corona virus there was a widespread increase in the use of Zoom. This also resulted in numerous reports of "zoombombing" (uninvited guests accessing and disrupting meetings), which combined with the lack of end-to-end encryption has left many doubts as to the adequacy of Zoom's privacy and security medhanisms.

3.4. Zoom pro-account (with monthly subscription) - seems to avoid some of the above issues.

3.5 Facetime provides video calling on Apple products but has been recently been subject to a bug that undermined the level of privacy; https://venturebeat.com/2019/02/01/apple-apologizes-for-group-facetime-privacy-issue-delays-software-update/ - so check software is to up-to- date before using.

3.6 Whatsapp
This is a popular social messaging application with video call available in the latest software up-date. Whatsapp claims to offer safety and security with end-to-end encryption see https://www.whatsapp.com/security/. However, by default your contacts can view your status, so you will need to ensure that phone numbers for participants are not saved in your contacts and/or you need to change the privacy settings on your phone.

See https://www.vice.com/en_uk/article/m7qwgx/what-is-the-most-secure-video-conferencing-software