UNIVERSITY OF SUSSEX

Guidance on the use of video conferencing platforms in research and ethics review

The Research Ethics and Integrity Committee recognises that video conference services permit important communications and interactions between researchers and participants that would not be possible otherwise[1]. This paper recommends principles of good practice that need to be applied in the use of these services in a way that is ethical, and both protects and reassures research participants and researchers.

By their nature, no platform is entirely safe, and researchers (and supervisors for students) need to undertake informed assessment as to the suitability of on-line platforms for the research and make reasoned choices when using them on a case by case basis.

The use of communication platforms and services by University researchers

All researchers (whether students or staff) are strongly advised to employ services for which the University has a subscription or contract for the processing of data. BSMS students should seek guidance specific to the Medical School.[2].

For video conferencing this is:

- Microsoft Teams
- Microsoft Skype for Business
- Zoom for Education

How each should be used is described below.

** The use of video conferencing services (such as Skype, Facebook Messenger, WhatsApp) using personal accounts is not recommended as they have* **not** *been evaluated as appropriate and approved for University business that involves processing personal data.**

Planning your research – evaluating the nature of personal data expected to be received

Researchers should refer to the University's *Information Security Policy - Information Handling* document[3] to ascertain whether the information to be received can be classified as either 'Confidential' or 'Strictly Confidential'. Data that falls outside of these definitions will be deemed 'non-sensitive'. The University

[1] This guidance does not include how such platforms as Twitter, Linkedin or Facebook are used for research. As a rule of thumb these services are permitted for publicising research (not for discussions or two way communications) if they have received approval through University ethics systems after presenting the precise text that will be used. Ethically, the principle of avoiding any confusion or potential of conflict of interest between the personal and professional/academic is essential.

[2] Student researchers within the Brighton & Sussex Medical School should consider the guidance provided from BSMS RGEC at https://www.bsms.ac.uk/research/support-and-governance/governance-and-ethics/covid-19-research-update.aspx as they make use of IT infrastructure from the University of Brighton. [3] University of Sussex Information - Security Policy Information Handling (2017) https://www.sussex.ac.uk/infosec/documents/isp07-information-handling-policy.pdf

expects that *all types of personal data* will be handled, managed and ultimately destroyed in accordance with legal requirements[3] and good research practice[4].

Proposed use of video conferencing platforms

Platform	Non-sensitive data	'Confidential'	'Highly Confidential'*
Microsoft Teams	✓	✓	✓
Microsoft Skype for Business	✓	✓	✓
Zoom for Education	✓		

*In some instances, if the research involves the exchange of data, information or beliefs that may place the participant in danger or at potential risk of reputational damage, it could be concluded that the use of a video platform is unsuitable and that a standard phone conversation or postponement of the interview until face to face contact is possible again would be safer.

This may be important if the participant is overseas or an environment where they be facing potential persecution or monitoring or if they are using IT facilities or a location for which data or their personal security cannot be guaranteed.*

Access to platforms

- **Staff** have access by default to Teams, Skype for Business and Zoom
- **PGR** and **PGT** students have access to Teams and Zoom
- **Undergraduate** students currently have access to Zoom. On a case by case basis, a request may be submitted to the Research Governance Team (Research Ethics, Integrity and Governance Administrators)[6] for the use of Teams for research

If researchers use Zoom for their research, it must be configured using all recommended ITS security settings applied to their University account and with most recent updates[7]. When accessing platforms and services off campus users are responsible for making sure that the networks that they use are secure (the

[3] University of Susses Data Protection Policy (2018) https://www.sussex.ac.uk/webteam/gateway/file.php?name=dataprotection-policy.pdf&site=76,
[4] https://www.sussex.ac.uk/webteam/gateway/file.php?name=code-of-practice-for-research-june-2018.pdf&site=377 [6] http://www.sussex.ac.uk/staff/research/governance/contacts_sreos_committees [7] http://www.sussex.ac.uk/its/help/guide?id=232

use of 'free wi-fi' for example is to be avoided), the PC or device used has updated anti-virus software and that both the device and the accounts accessed through it have secure passwords. The National Cyber Security Centre (associated with CGHQ) provides useful guidance in this regard - (https://www.ncsc.gov.uk/section/advice-guidance/all-topics)

To keep staff teaching and research activity separate, the Research Governance team recommends the general use of **MS Teams** for research interviews and collaborative interactions.

Requirements for approval through the Ethics Review Process

Researchers should reflect on the ethical implications of using online platforms for communication and ensure transparency in communicating to potential participants how communication will occur.

The ***Participation Information Sheet*** should indicate:

- The platform to be used and a link to the provider's security statement[5]
- Whether the researcher intends to record the interview or conversation
- A link to the University's Data Protection policies - http://www.sussex.ac.uk/ogs/policies/information/dpa/privacynotice The Consent statements should include:
- an explicit statement consenting to interview via the named platform and to the audio recording of the conversation (where appropriate)To avoid excessively lengthy or complex Information Sheets, researchers can 'nest' some information or make it clearly available through a webpage published on the University's website.

Amendments

The arrangements for the use of the platform and the management of resulting data should be clearly indicated in the ethical review application. Any changes to the platform, the Participant Information Sheet or arrangements for the management of data should be submitted to the initial approver in the form of an **amendment**.

Recording interviews

It is advised that researchers should avoid the using functionality built into platforms to record interviews and instead use a separate device (such as an audio-recorder) that has a secure password. Where this cannot be avoided, help should be sought from ITS to understand the default location where this information is stored so that it can be retrieved and stored securely.

[5] Microsoft - https://www.microsoft.com/en-us/trust-center. Zoom - https://zoom.us/docs/en-us/privacy-and-security.htm – Please bear in mind that the exact location of these documents may change

The resulting file/files should be removed and **deleted** from the device or file location and kept securely in University approved research storage ('G: drive', OneDrive or Box). It is good research practice to fully delete recordings when transcriptions and note-taking is complete. If this is not possible given the nature of the research, participants should be clearly informed of the fact.

Files containing data that is classified as 'Confidential' or 'Highly Confidential' should be ***password protected*** within a specific folder or by using a file archive manager such as 7-Zip[6].

Further guidance about the ethical implications of internet mediated research

Association of Internet Researchers (https://aoir.org/) – Ethics - https://aoir.org/ethics/

The British Psychological Society (https://www.bps.org.uk/) - Ethics Guidelines for Internet-Mediated Research (2017) - https://www.bps.org.uk/news-and-policy/ethics-guidelines-internet-mediated-research2017

UK Research Integrity Office (https://ukrio.org/) - internet-mediated research (2016)

https://ukrio.org/new-guidance-from-ukrio-internet-mediated-research/

Approved by Research Ethics and Integrity Committee - 6 May 2020

[6] http://www.sussex.ac.uk/its/services/software/list?filter=home_use&id=17

Appendix – Email of 28 April to all Support Staff -'Staying safe when meeting online'

Staying safe when meeting online

Dear all staff,

Due to the advent of Covid-19, and in keeping with most higher education institutions across the world, the University of Sussex has rapidly had to review the way it works in order to maintain service standards. At the heart of this has been the swift implementation of new software designed to allow staff and students to collaborate when away from campus:

- Skype for Business (part of Office 365) has been deployed to all staff ensuring that external telephone services are available to everybody who downloads the software

- Microsoft Teams (also part of Office 365) has been rolled out to staff to aid internal video calling and meetings and to provide a forum for shared working on documents in real-time. Teams should also be used to facilitate video/voice calls where the discussion is likely to include commercial-in-confidence or highly sensitive (research) material. External collaborators can be invited into a Teams site or Teams call

- Zoom Education has been implemented for all staff and students to aid live teaching, in tandem with the Panopto video platform. Zoom is also suitable for external meetings that do not involve commercial-in-confidence or highly sensitive information.

Full details of how to download and safely use each of these products can be found on the IT Services (ITS) web pages.

In parallel with our introduction of these tools there has been significant media coverage about technology concerns and cyber security threats. Understandably, given the huge surge in its use, Zoom has been referenced in many of these articles. So it's important for me to address this and reassure our community why ITS still sees Zoom as the best tool for us in these circumstances.

At Sussex, we have Zoom Education licensing which has enhanced security and compliance - as opposed to the basic, freely downloadable version of the app. This is why we asked all users to

transfer over to their Sussex account recently and use their normal IT sign-on and password used for all Sussex accounts (known as Single-Sign-On).

As with any software, privacy and security are a joint responsibility of the software provider, ITS as administrators and you as the user. Many of the recent press articles which highlight where there have been issues are because the user isn't aware of how to help protect their own privacy and security. So, we want to make sure you have all the information you need to make these decisions:

- All users should install software updates as soon as they are available (when working at home – computers in the office are updated automatically)
- Meeting hosts should set their accounts to provide the highest protection for the privacy of all meeting participants in accordance with the published guidance
- All users should be using their IT log in and password to log into and use Zoom
- All users should periodically check the ITS published guidance for updates

In light of the negative press, Zoom has addressed criticism over its privacy and cybersecurity features head on. Please see the letter I received from the Zoom Executive Team late last week. I received further information from Zoom today that encryption functionality will also be released on 30 May to provide even greater security improvements.

The ITS and TEL teams at the University constantly monitor the security of all of our software, and over the past 12 months we have taken huge strides in strengthening our defences. That being said, criminals are continually seeking new ways to exploit us. Vigilance and effective password management are the best defences that any of us can demonstrate to safeguard ourselves.

As the University continues to improve its online learning capacity, privacy and security remain a top priority and we will continue to address any concerns that are raised. ITS and TEL have issued comprehensive guidance for users and delivered webinars to show how Zoom can be used effectively and safely. We'll keep our guidance up to date based on any new findings or best practice. With the security measures that we have in place - and the ongoing security enhancements the company is making - we believe that Zoom is the most appropriate videoconferencing platform for teaching remotely that is available on the market today.

Kind regards,

Jason Oliver
Director of IT

Sent by

Internal Communications, University of Sussex