**The following advice has been collated from various sources including the Library, Information Services, Data Management and Research and Innovation Services.**

We advise that researchers don’t use a tool for confidential data until they can demonstrate that they can comply with GDPR requirements and follow the University’s guidance on handling confidential data.

**Data storage**

For data storage, the simplest way to do this is to use the **Office 365** tools provided by the University. Confidential data should be stored on secure servers as per the Information Security Team’s guidance, so that rules out most free cloud tools like Google Docs./Drive etc.

**If a researcher isn’t sure whether a tool is appropriate they should seek advice from their local research ethics committees, Data Management, (**research-datamanagement@glasgow.ac.uk) **and/or the Data Protection and Freedom of Information (**dp@gla.ac.uk**) teams.**

**Questionnaires/Surveys**

For **Staff, PGR, PGT and UG** students the preferred survey option is Qualtrics - <https://www.gla.ac.uk/myglasgow/it/softwareandonlinetools/qualtrics/>. We offer and recommend Qualtrics as a good, GDPR-compliant, high-functionality, option.

However, we recognise that sometimes another GDPR-compliant platform may be preferable; examples of reasons for this may include ease of access regarding geographic locale and restrictions on software access, cross-institutional collaboration among others.

If another platform is used, there should be a brief justification for the platform’s use and clear evidence that is GDPR compliant provided in any ethics application.

**Data security when collecting data using digital methods**

Recordings (either audio or audio-visual) must be encrypted as soon as is reasonably possible and stored on an encrypted drive or laptop.

For **Zoom** users shouldsign in using the University of Glasgow email. They should log in at <https://uofglasgow.zoom.us> with the domain **uofglasgow.** Recording should be done on the local computer rather than the cloud. In addition, and if relevant, any automated backups of audio or audio-visual files stored in the User Account must be deleted immediately once files are downloaded and encrypted.

**WhatsApp**- secure but difficulty recording - so would need to record separately – you may require one of these for a digital voice recorder - <https://www.dictaphones.co.uk/Olympus-TP-8-Telephone-Pick-UP-p/v4571310w000.htm> - these also work for any telephone based interviews. There are also Apps to allow WhatsApp recording however you should check their privacy policy and **ensure recordings are not saved to the cloud and only on the user’s device** – whatever method is used the guidance about encrypting and removing the audio files from your device/phone and storing securely above still holds.

Informed consent (verbal or written) **must be obtained** and methods to achieve this clearly stated and evidence of consent retained.

If files containing confidential data must be transferred to other team members, then the guidance on confidential data should be followed to ensure security and GDPR compliance. For information on encryption please see the guidance here:

<https://www.gla.ac.uk/myglasgow/it/informationsecurity/confidentialdata/>

Other platforms such as Signal and Threema and WeChat should only be used where GDPR compliance is clear.

<https://gdpr.eu/compliant-services/>

see also [www.signal.org](http://www.signal.org)

and <https://threema.ch/en>

and <https://www.wechat.com/> **see also** <https://www.westminsterpapers.org/article/id/274/>

End\_\_\_\_\_\_