**Data Management Plan Guidance**

Before following this plan, all group members must have completed the [Data Protection Training](https://www.ed.ac.uk/records-management/training/data-protection) on LEARN. To access, log in to Learn using your UUN and your EASE password. Within Learn, find the [Self Enrol] tab, near the top of the page. Scroll down or search for the Data Protection Training. To enrol on the course, select the enrol button, then press ok. Once enrolled, this course will appear on your Homepage next time you log in.

**Devices for Storage and Collection**

Below is a list of options fro securely storing your collected data. They are:

* Encrypted personal Mac – [instructions](https://www.ed.ac.uk/infosec/how-to-protect/encrypting/encrypting-computer-laptop/encrypting-apple-computers)
* Encrypted personal Windows – [instructions](https://www.ed.ac.uk/infosec/how-to-protect/encrypting/encrypting-computer-laptop/encrypting-windows-computers)
* Encrypted personal Linux - [instuctions](https://www.ed.ac.uk/infosec/how-to-protect/encrypting/encrypting-computer-laptop/encrypting-linux)
* DICE account
* University Computing Account.
* Encrypted Smart Phone - [instructions](https://www.ed.ac.uk/infosec/how-to-protect/encrypting/encrypting-smartphones-and-tablet-devices)

**Data Collection**

**What data will you collect?**

**Audio** – This data type should be gathered by a recording device, which is not connected to a web storage service, ie iCloud. Once the recording has been made, the file is to be transferred over to the encrypted laptop or container. If transcribing the recordings, you must do so yourself (i.e No Outside Services), with any personal information removed and anonymised.

**Video/Pictures** – This data type should be recorded and stored, with no connection to online storage service, ie. iCloud.. The data should then be transferred to your storage device, and personally transcribed if you choose to do so. While capturing this data, reduce taking images of participant’s faces to reduce identifiable information.

**Personal Notes –** This type of data does not need to be encrypted or protected, as long as there is no identifiable Personal Information taken down. If you do capture this, please store on an encrypted device, and anonymise the notes

**Survey/ Questionnaires**

If you choose to perform surveys and questionnaires, you must not run using Non-GDPR compliant services. For example, you may not use Google Sheets. We would suggest that you write the questionnaire and collect data through pen and paper. This data should then be collected and catalogued on an encrypted device.

**How much data will be generated?**

0-50GB – you will be very unlikely to collect and store more data than 50GB. Please keep the amount of data collected to a minimum ie Collect only what you need to perform your evaluation.

**Data Management**

**How to present the Data?**

Each participant will be given a unique identifier, and any metadata or documentation should be sufficient for you and your team members can manage the records captured. If you use quotes from participants, please refer to the unique identifier in your final report.

**Where will the data be stored and backed-up?**

You are to store the data you have collected in your chosen device from the list given above. This device will also be password protected.

**How do you share data amongst Group Members?**

If the data is to be shared, you will use university services such as SharePoint and not Google Docs/Sheets. You may also share data through your University Email as an attachment. Do not use private email addresses, such as Gmail.

**Which data do you plan to keep and for how long?**

All data records should be deleted by the end of the semester. You are not to keep any of the data collected beyond this end date.

**Which data will be shared and how?**

The data you have collected is for you, and your team’s use alone. Data may only be shared with participants, who ask to see the data you have collected from them.