Undergraduate Dissertation – Data Protection Guide and Requirements

If your research involves personal data you must ensure that you take every precaution to protect it and keep it secure. Undergraduate and Taught Postgraduate students collecting and processing the personal data of research participants will be doing so for their own personal reasons/purposes - the University is not the Controller for this information.

Personal data is information from which an individual can be identified, from that information, or in combination with other information.

If you would like to learn more about what personal data is and how to keep it secure you can visit the website of the UK Information Commissioner Full guidance on data protection and research is available online here: https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/ProcessingDataforResearch.aspx

Privacy Notices

It is good practice to provide a Privacy Notice to research participants if you are collecting personal data from them. This tells them what data you are collecting, why you are collecting it, who it will be shared with, how it will be stored and when it will be destroyed. The Privacy Notice template can be found with the Participant Information Sheet.

When to provide the Privacy Notice:

- Data collected directly from participants – provide Privacy Notice at the time of collection e.g. with the Participant Information Sheet.
- Data collected by a third party – provide data subjects with a Privacy Notice within 30 days of you receiving the data, unless this would involve 'disproportionate effort' or would be impossible. Find out from the third party whether they provided a Privacy Notice to the data subjects. If it is disproportionate/impossible, keep a record of why this is the case.
- Data collected in a public place, e.g. a transport survey – in these situations where provision of a Privacy Notice is not appropriate/possible you must consider placing posters in the general vicinity to inform the public.

Data Sharing

You must not share the personal data you collect with anyone other than your Supervisor and other Academic staff who are responsible for reviewing/assessing your dissertation, only if strictly necessary. It may be required to verify the findings of your study.

Data Storage

For your own protection and to avoid having any issues if personal data you have collected or the device you are storing it on is lost or stolen you must ensure that all your own devices that you are using to process personal data are encrypted and have anti virus protection(this is available free from the University).

Do *not* label files containing personal data with the research participant's name. You should give each participant a unique number and keep a list linking those numbers to research participant's names in a secure password protected file to which *only you* have access.

Ensure files/documents containing personal data are password protected.

If you think the nature of your research requires you to use a portable device (such as a Dictaphone) you must discuss this with your Research Supervisor. Any portable device must be encrypted.

If you are keeping research participant's personal data in paper format this must be kept under lock and key at all times.

If you are intending to use any third party services, apps, or software check that they are reputable and provide privacy notices and information about the security measures they use to protect data processed by their services. If they don't have this information it is likely that they are neither reputable nor secure. If you are using your smart phone to store data check that other apps you have downloaded are not accessing participant personal data. Often when you sign up to an app they ask for permission to access your contacts, photos, etc. in to provide services – if they are also accessing your files then you may have to remove them. You can check out the possibility of having a secure SD card on your phone which these services can't access – or use another device for collecting and storing personal data (this section links to the next one).

Use of personal/portable devices

This includes laptops, tablets, mobile phones, USB/flash drives, DVD's, CD's, Dictaphones, cameras, etc. – anything that could be lost/stolen and accessed by someone else.

Any portable device which is used to record research participant's personal data MUST be encrypted.

It is good practice to secure all your devices with a password or pin number for your own protection.

Anonymisation

Data must be anonymised as soon as possible. Anonymising data is not straightforward and can be complicated, therefore always have someone else check to confirm for you. The Information Commissioner's guide to anonymization can be found online using the following URL: https://ico.org.uk/media/1061/anonymisation-code.pdf

Data Disposal

You must dispose of personal data securely when it is no longer required. The retention period will have been set out in your Privacy Notice and will normally be until the end of the examination/assessment process. Any hard-copy data must be disposed of by shredding it with a fine cross-cut shredder – don't use a strip shredder (https://www.youtube.com/watch?v=Rfw8FIIf8zU). If you have used a personal/mobile device delete the documents/information and then delete again from your recycle bin. When you get rid of the device at the end of its life you should ensure it is completely wiped. The ICO provides guidance here: https://ico.org.uk/your-data-matters/online/deleting-your-data-from-computers-laptops-and-other-devices/