DMP Guidance

business or other organisation. Examples include commercially confidential information, and sensitive location details (e.g. relating to endangered species, military sites, etc.).

Research data is information collected to answer a research question. Where the data have been collected from research participants, they are usually processed at some stage in the research to remove direct identifiers such as names and contact details, although they may still include indirect identifiers (such as key codes, age, job title, etc.). De-identified research data is generally suitable for public sharing, although care may need to be taken to unlink pseudonymous key codes and mask or remove indirect identifiers before making research data widely available.

Anonymous data is data that no-one can relate to an identifiable individual. For example, if a survey did not record any information relating to the identity of an individual, including data such as an email address or telephone number, then the data collected could be described as anonymous, providing that the information itself was not sufficiently detailed enough to

- locations for storage of non-digital data, e.g. signed consent forms, paper questionnaires, such as a locked cabinet in a locked office on University premises. Consider storage in the field/in transit as well as on University premises.

For each location, indicate whether it will be used to store/process identifying information or de-identified research data, and provide details of access controls that will be applied, such as password protection, or encryption of files or devices.

3.2 Risk management

Describe any administrative measures that you will take to control the risks of inappropriate disclosure of personal data/confidential information. These might include:

- encrypting any hardware that will be used to store such data (such as audio-recording devices and laptops) and deleting data from these devices as soon as they have been transferred into the primary storage location. Storage on external devices should be avoided as much as possible and should always be temporary;
- digitising hard copy data, including consent forms, for secure digital storage, and destroying paper originals. Consider using digital consent methods where possible: for example, the University's REDCap platform provides an e-consent function;
- storing hard copy data, including consent forms, in a locked cabinet in an office on University premises that is locked when not in use;
- storing participant records separately from research W*nBT/F[<)]TJETQ0.rgon

using of a locked cabinet within an office that is locked when unattended. Unnecessary duplication of personal data should be avoided. Where possible, signed consent forms should be held in secure electronic storage: paper forms can be scanned and destroyed if there is no good cause for retaining the paper originals.

See the RDM web pages for guidance on data storage and information security, and online survey tools (bottom of page).

Most research data collected from research participants can be safely and ethically

A sample consent form, with consent formulae for sharing of anonymised open data, and for restricted sharing of data under safeguards, can be found on the

Guidance on the retention of personal data can be found in Data Protection for Researchers.