TEMPLATE FOR A DATA MANAGEMENT PLAN

The following **template** should be used to develop a Data Management Plan (DMP) to accompany a research proposal. The notes (*in italics*) provide further context and guidance for its completion. Where substantial data is generated from the research, the DMP will be more in depth and therefore likely to be 2 or 3 pages long for low impact studies generating small amounts of data, DMPs will be short ie less than half a page.

Comment test is the University standard response, if you are going something different this must be updated to reflect the actual activities.

0. Proposal name

Exactly as in the proposal that the DMP accompanies

1. Description of the data

1.1 Type of study

Up to three lines of text that summarise the type of study (or studies) for which the data are being collected.

1.2 Types of data

Types of research data to be managed in the following terms: quantitative, qualitative; generated from surveys, clinical measurements, interviews, medical records, electronic health records, administrative records, genotypic data, images, tissue samples,...

1.3 Format and scale of the data

File formats, software used, number of records, databases, sweeps, repetitions,… (in terms that are meaningful in your field of research). Do formats and software enable sharing and long-term validity of data? https://www.ukdataservice.ac.uk/manage-data/format/recommended-formats.aspx

MS office document and PDF in the dissemination of the research

2. Data collection / generation

Make sure you justify why new data collection or long term management is needed in your Case for Support. Focus in this template on the good practice and standards for ensuring new data are of high quality and processing is well documented.

2.1 Methodologies for data collection / generation

How the data will be collected/generated and which community data standards (if any) will be used at this stage.

2.2 Data quality and standards

How consistency and quality of data collection / generation will be controlled and documented, through processes of calibration, repeat samples or measurements, standardised data capture or recording, data entry validation, peer review of data or representation with controlled vocabularies.

3. Data management, documentation and curation

Keep this section concise and accessible to readers who are not data-management experts. Focus on principles, systems and major standards. Focus on the main kind(s) of study data. Give brief examples and avoid long lists.

3.1 Managing, storing and curating data.

Briefly describe how data will be stored, backed-up, managed and curated in the short to medium term. Specify any community agreed or other formal data standards used (with URL references). [Enter data security *standards in Section 4].*

Research data will be stored on the University's X:drive/V:drive. University-managed data storage is resilient, with multiple copies stored in more than one physical location and protection against corruption. Daily backups are kept for 14 days and monthly backups for an additional year.

Commented [RL1]: University standard response, if you are going something different this must be updated to reflect the actual activites.

3.2 Metadata standards and data documentation

What metadata is produced about the data generated from the research? For example descriptions of data that enable research data to be used by others outside of your own team. This may include documenting the methods used to generate the data, analytical and procedural information, capturing instrument metadata alongside data, documenting provenance of data and their coding, detailed descriptions for variables, records, etc.

All research data will be organized as per the Universities metadata standards http://staff.napier.ac.uk/services/research-innovation-office/research-data/Pages/Organising.aspx

Commented [RL2]: University standard response, if you are going something different this must be updated to reflect the actual activites.

3.3 Data preservation strategy and standards

Plans and place for long-term storage, preservation and planned retention period for the research data. Formal preservation standards, if any. Indicate which data may not be retained (if any).

The Edinburgh Napier Data Management Policy requires research data to be retained after project completion if they substantiate research findings, are of potential long-term value or support a patent for at least 10 years. The policy also requires that funders and/or sponsors requirements are met. Long term storage is provided through the University data repository.

Consent forms can be kept for up to 6 years after the project ends as allowed by the Prescriptions and Limitations Act e.g. as evidence if someone comes back to say they never consented.

Other personal data including audio-visual/audio/visual data should be destroyed once any audit for verification of the findings has taken place and within 12 months of the end of the project.

Commented [RL3]: University standard response, if you are going something different this must be updated to reflect the actual activites.

Commented [RL4]: remove if you are not collecting this data

4. Data security and confidentiality of potentially disclosive information

This section MUST be completed if your research data includes ***personal data relating to human participants in research****. For other research, the safeguarding and security of data should also be considered. Information provided will be in line with you ethical review. Please note this section concerns protecting the data, not the patients.*

4.1 Formal information/data security standards

Napier University meets the Cyber Essential standards for data stored in the X:Drive/V:drive.

Commented [RL5]: University standard response

4.2 Main risks to data security

All personal data has an element of risk. Summarise the main risks to the confidentiality and security of information related to human participants*, the level of risk and how these*

risks will be managed. Cover the main processes or facilities for storage and processing of personal data, data access, with controls put in place and any auditing of user compliance with consent and security conditions. It is not sufficient to write not applicable under this heading.

MRC guidance on the Confidentiality and data security is provided

When collecting and transferring data to X:Drive/V:Drive or sharing with collaborators the risks and mitigations are:

Commented [RL6]: update as appropriate

5. Data sharing and access

Identify any data repository (-ies) that are, or will be, entrusted with storing, curating and/or sharing data from your study, where they exist for particular disciplinary domains or data types. Information on repositories is available here.

5.1 Suitability for sharing

Is the data you propose to collect (or existing data you propose to use) in the study suitable for sharing? If yes, briefly state why it is suitable.

If No, indicate why the data will not be suitable for sharing and then go to Section 6.

Data generated by the project (identified above) will be made open once appropriate changes have been made to honour assurances of confidentiality and anonymity.

Commented [RL7]: University standard response, if you are going something different this must be updated to reflect the actual activites.

Where data may not be freely available the metadata only will be made available in the repository and the datasets available on request and subject to a data sharing agreement

5.2 Discovery by potential users of the research data

Indicate how potential new users (outside of your organisation) can find out about your data and identify whether it could be suitable for their research purposes, e.g. through summary information (metadata) being readily available on the study website, in the MRC gateway for population and patient research data, or in other databases or catalogues. How widely accessible is this depository?

Indicate whether your policy or approach to data sharing is (or will be) published on your study website (or by other means).

Datasets will be allocated a DOI and stored on our open access Research Repository in accordance with the University research data deposit process.

Commented [RL8]: University standard response, if you are going something different this must be updated to reflect the actual activites.

5.3 Governance of access

Identify who makes or will make the decision on whether to supply research data to a potential new user.

For population health and patient-based research, independent oversight of data access and sharing

Indicate whether the research data will be deposited in and avail ate how able from an identified community database, repository, archive or other infrastructure established to curate and share data.

Not required when data is fully open. Where data may not be freely available a decision to share will be made jointly between the PI and the University data access panel

Commented [RL9]: University standard response. update is you are doing something different

5.4 The study team's exclusive use of the data

Funders have a requirement for timely data sharing, with the understanding that a limited, defined period of exclusive use of data for primary research is reasonable according to the nature and value of the data, and that this restriction on sharing should be based on simple, clear principles. What are the timescale/dependencies for when data will be accessible to others outside of your team? Summarize the principles of your current/intended policy.

Researchers will have exclusive use of the data prior to publication

5.5 Restrictions or delays to sharing, with planned actions to limit such restrictions

Restriction to data sharing may be due to participant confidentiality, consent agreements or IPR. Strategies to limit restrictions may include data being anonymised or aggregated; gaining participant consent for data sharing; gaining copyright permissions. For prospective studies, consent procedures should include provision for data sharing to maximise the value of the data for wider research use, while providing adequate safeguards for participants. As part of the consent process, proposed procedures for data sharing should be set out clearly and current and potential future risks associated with this explained to research participants.

Restrictions may be due to the confidentiality and anonymisation of the data.

Commented [RL10]: University standard response. update is you are doing something different

5.6 Regulation of responsibilities of users

Indicate whether external users are (will be) bound by data sharing agreements, setting out their main responsibilities

Where data may not be freely available the metadata only will be made available in the repository and the datasets available on request and subject to a data sharing agreement

Commented [RL11]: University standard response. update is you are doing something different

6. Responsibilities

Apart from the PI, who is responsible at your organisation/within your consortia for:

- *study-wide data management*
- *metadata creation,*
- *data security*
- *quality assurance of data.*

The first point of contact for all queries in relation to this data is the PI. Who will also have overall responsibility for the production and maintenance of metadata. Preparation and upload of the data will be carried out by the team with the support of the University's Information Services staff.

Commented [RL12]: University standard response, if you are going something different this must be updated to reflect the actual activites.

7. Relevant institutional, departmental or study policies on data sharing and data security	
Please complete, where such policies are (i) relevant to your study, and (ii) are in the public domain, e.g. accessible through the internet. *Add any others that are relevant*	
Policy	**URL or Reference**
Data Management and Sharing Policy & Procedures	*https://staff.napier.ac.uk/services/research-innovation-office/research-data/Documents/Research%20Data%20Management%20Policy%202022.pdf*
Data Security Policy	*http://staff.napier.ac.uk/services/cit/infosecurity/Pages/InformationSecurityPolicy.aspx*
Data Sharing Policy	*http://staff.napier.ac.uk/services/secretary/governance/DataProtection/Pages/DataSharing.aspx*
Data Protection for Research	*https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/ProcessingDataforResearch.aspx*
Other:	
Other	
8. Author of this Data Management Plan (Name) and, if different to that of the Principal Investigator, their **telephone & email contact details**	