IMPS

Introduction

This is a guide to the assessment of data management plans (DMPs) submitted as part of applications for ethical review. It is provided for use by members of School Research Ethics Committees (SRECs) that have implemented a DMP requirement.

The guide has been prepared by Information Management and Policy Services (the Data Protection Office) and the Research Data Manager, and is based on the procedure established for the University Research Ethics Committee (UREC).

The guide includes:

- an outline of the process for assessment of DMPs as part of the research ethics review;
- guidance on data protection, the common law duty of confidentiality, participant information sheets (PIS) and consent forms, data security, pseudonymisation and anonymisation of personal data, and the preservation and sharing of research data;
- a DMP assessment checklist;
- an Appendix of references.

Purpose of the data management plan

The purpose of the data management plan is for the applicant to demonstrate that he/she has planned appropriately for:

- the processing of any *personal data* that will be collected in the research in Information Compliance policies;
- the preservation and (wherever possible) sharing of any *research data* that will Research Data Management Policy.

Information provided in the DMP about how data will be managed must be appropriate

Where the DMP gives rise to serious concerns or the SREC requires guidance on specific questions, advice is sought from the Data Protection Office, the Research

The identity and contact details of the Data Controller (the University of Reading);

The contact details of the Data Protection Officer;

Consent to participate is required to ensure ethical research practices. A research project consent form is primarily concerned with consent for ethical purposes and may include statements to ensure the participant fully understands the nature of study they are taking part in, and their right to withdraw from the study at any time.

But if researchers wish to seek permission to include the participant in a register and/or be contacted about other research studies in the future, this should also be included on the consent form.

IMPS have produced a template consent form that can be used as guide.

Consent forms should *not include* statements such as:

Surveys

The participant s consent is not required for these purposes and consent forms should avoid specification of unnecessary restrictions to the data processing.

If there is information about *how the researcher will handle or share the data*, this should be included in the PIS. The consent form should include a statement to confirm that the participant *understands* how their data will be used. There is suggested wording for this statement in the IMPS template consent form.

The consent form should include a statement to indicate that the participant has understood the research data collected from them will be preserved and shared, in line with the information provided in the PIS.

Data security

On-site storage in existing University-managed services (for example, OneDrive/ Office365 or a location on the local network) should be used wherever possible.

Researchers should be *encouraged* to avoid external hardware (for example, USB sticks or external hard drives) for the processing of personal data wherever *possible*. External hardware can present greater risks of loss, theft, corruption, or unavailability due to lost or forgotten passwords or an absence of secure and separate backup.

Where the researcher deems use of external hardware *essential* (and reasons may vary, from file/data size needs, to practicalities of remote working or ability to transfer data) it *must be encrypted*. Guidance is provided in the Encryption Policy.

Personal data held in hard copy, such as paper consent forms, *can* be stored digitally

there is no need to store *both* hard copy and digital. Where hard copies *are* stored, IMPS

with limited access to researchers, *within* an office that is locked when unoccupied. During remote working, a location out of sight of the household (ideally locked), in a secure property may be the best minimum possible. When data are stored digitally on University networks, requiring a staff password (and multi-factor authentication where applicable) will be sufficient, providing access to the data is strictly limited and controlled.

If applicable - and for the vast majority of projects this will not be where personal data is to be published or made widely available to others outside the University, assurances around security should not be made. We cannot make meaningful assurances about security for data made available publicly that could be accessed or reused by anyone.

If a project involves the recruitment of research participants, care must be taken to

participant email addresses to other participants, are common.

Where personal data is to be stored long term, the researcher must consider how it will be managed should they leave the University - for example, by arranging handover to a relevant permanent member of staff or the Head of School.

which does not relate to an individual, is *not covered by data protection law*.

Pseudonymising data is a very good *security and personal data minimisation method* but does not make the data anonymous.

In the majority of cases, the lifecycle of participant data is:

Personal data is collected;

The data is coded/de-identified/assigned a unique number where this data could still be matched back to the participant (typically by means of a table that links the unique code to the individual participant), it should be treated as
;

Findings from the study are presented in anonymous form, with the linked unique code removed from any data (which enables publication of results with no risks of identification to participants).

IMPS ask

It is possible within data protection law to maintain and provide access to identifiable

, *providing* researchers are transparent about who the data may be shared with, and for what purpose, and as long as appropriate safeguards are in place - for example, the data are held in a repository that provides a controlled access procedure.

Consent procedures should not preclude sharing of research data. Researchers should not set a time limit on the retention of the research data collected from participants, or state that all data will be destroyed at the end of the project, or undertake that data will not be shared outside of the project. Such undertakings are not required, and will prevent researchers unnecessarily from making their research data accessible to others, even if they have been anonymised.

Contacts

stath(p)-5(r4n W* 8(fr-FRa))] TJ ET O EMC /Spa 10(e) xstath(p)-5(r5n W* 8(fr-FRa))] TJ E

Appendix. References to key resources

DMP template for participant-based research

https://www.reading.ac.uk/research-services/research-data-management/data-management-planning/research-ethics-and-data-protection

The template that must be used for submission of the data management plan with the application for ethical review. Section-by-section guidance on completing the DMP is also provided.

Data Protection for Researchers

https://www.reading.ac.uk/imps/data-protection/data-protection-and-research

Detailed guidance on all aspects of personal data processing in research. Includes a sample consent form and data protection information for participant information sheets.

Information Compliance policies

https://www.reading.ac.uk/imps/information-compliance-policies

Includes policies on: Data Protection, Encryption, Bring Your Own Device, Remote and Mobile Working, and Information Security incident Response.

Research Data Management Policy

https://www.reading.ac.uk/research-services/research-data-management/about-research-data-management/research-data-management-policy

that substantiate published research outputs.