DMP assessment guide for School RECs

Contents

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 accordance with data protection laws and the University's Information Compliance policies;
- the preservation and (wherever possible) sharing of any *research data* that will support published research findings, in accordance with the University's Research Data Management Policy.

Information provided in the DMP about how data will be managed must be appropriate and consistent with the information to be provided to participants in the PIS and consent form, and with any discussion of data management elsewhere in the application.

Process

- A DMP is completed by the applicant using the DMP template for participant-based research, with reference to the accompanying guidance document, and included with the application for ethical review that is submitted to the SREC;
- The DMP, participant information sheet and consent form are reviewed by members of the SREC with reference to the guidance and checklist provided in this document;

- 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 Data Manager, or the Secretary to UREC, as relevant;
- Further to deliberation by the SREC, any conditions that must be met for the application to receive a favourable ethical opinion, along with any advisory comments, are recorded in the SREC response to the applicant.

Data protection

This guidance highlights key points to consider relating to the processing of personal data. It is not intended to be exhaustive. More information can be found in the Data Protection for Researchers guide.

'Processing' refers to all activities involving personal data, including the collection, storing, analysing, sharing, retention and deletion of data.

'Personal data' refers to any data that relates to a living individual and includes pseudonymised and coded data where this relates to an individual, for example via a unique identifier.

'Special Category data' refers to sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a person's sex life or sexual orientation.

Data protection laws set out legal obligations on *Data Controllers* to protect personal data and ensure that it is handled lawfully, fairly, transparently, securely and for no longer than is necessary.

In most cases, the *Data Controller* for research activities performed by those working under the auspices of the University is the *University of Reading*.

Common law duty of confidentiality

The Common Law Duty of Confidentiality is not changed by Data Protection Laws. Researchers will still need to give due regard to the duty of confidence when collecting, storing and sharing confidential information.

Participant information sheets

Data protection law mandates that specific information is provided to the individuals at the point personal data is collected, or prior to that processing taking place. This is often referred to as a 'Privacy Notice' or 'Fair Processing Notice'. For research participants, this information is most logically included in the participant information sheet (PIS).

By law, privacy notices must contain the following (those most commonly relevant to research are listed):

- The identity and contact details of the Data Controller (the University of Reading);
- The contact details of the Data Protection Officer;
- The lawful basis for the processing (under data protection laws);
- Notice of the individual's rights under data protection laws;
- The right to lodge a complaint with the Data Protection Supervisory Authority (for the UK, the Information Commissioners' Office).

IMPS provide advice on data protection information to be included in the participant information sheet, which can be used to cover these requirements.

In addition to the above, the information listed below must also be included. As the details will vary on a project-by-project basis, the suggested wording in the template will need to be supplemented by the researcher to cover:

- The purposes of the data processing (the nature of the study and what it will be used for);
- The individuals or *categories* of people the data will be shared with (for example, research staff of the university, researchers at the University of X, partners at the NHS);
- Whether any *personal data* will be sent outside of the EEA to a third country (known as a restricted transfer) and what safeguards will apply. **Note:** For projects which are subject to collaborative agreements or contracts and involve the transfer of personal data to other international organisations, advice should be sought from Research and Enterprise Services, as in many cases the safeguard will be additional *Standard Contractual Clauses*;
- The retention period for the personal data, or, where this may be undefined or open ended, the process that will be followed to determine if it is still required (for example 'for the life of the study' if strictly needed, 'until it can be anonymised', or 'until it is reviewed and no longer required for research purposes'). **Note:** Data protection laws do not stipulate any specific timeframes for when data must be deleted. Researchers should avoid giving commitments to destroy personal data by a given date, and should be clear that any retention limitation applies to *personal data only*, not to *anonymised research data*, which may be retained indefinitely and will be subject to the University's data preservation and sharing policy.

Participant information sheets should also clearly address the researcher's plans for preservation and sharing of the research data collected from participants in support of research findings. In most cases research data will be *anonymised* for public sharing. A suitable statement would be: 'The information we collect from you will be preserved and made publicly available in anonymised form, so that they can be consulted and re-used by others'.

There are limited and qualified exemptions from some of the above requirements within data protection law, for example, where delivery of the above information would be impossible (e.g. where we have no direct relationship with the subjects of the data and may be making secondary uses of existing research data), or where meeting the above requirements would seriously impair or prejudice the objectives of the study. This is not the case with the majority of the research undertaken by the University, would be *by exception*, and would not apply for reasons of mere inconvenience or because of fears that that people may be discouraged from taking part. The Data Protection Office should be consulted if any grounds for using an exemption are being considered.

It is possible to share identifiable data, or anonymised data where there is a higher risk of re-identification, for example by being linked with existing data, providing:

- the researcher is transparent with the data subjects about how their data will be disclosed to others;
- in the case of identifiable data, it is for a purpose compatible with the original purpose for which the data was collected (e.g. for non-commercial research);
- there are suitable safeguards around the data sharing, for example, procedures to confirm that the recipient of the data is a member of a legitimate research organisation, and provision of the data under a data access agreement setting out the recipient's responsibilities to process the data securely. Some data repositories, including the University's Research Data Archive, can provide controlled data sharing mechanisms for identifiable and higher-risk anonymised data. See the section on data preservation and sharing for more information.

For sharing of data that is identifiable or carries a higher risk of re-identification, a suitable statement would be: 'The information we collect from you in this study will be preserved, and subject to safeguards will be made available to other authenticated researchers'.

Consent and consent forms

In data protection terms, for the vast majority of research activities, the lawful basis relied on by the University for the processing of personal data is *not* 'with consent'. In most cases the lawful basis will be 'public task'.

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:

- ‘I consent to Researcher X collecting/storing my data’
- ‘I consent to Researcher X sharing my data with their supervisor/research assistants’
- ‘I consent to my data being destroyed after 5 years’
- ‘I consent to my data being stored on University OneDrive/collected via Online 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 and, unless there are project specific requirements for retaining ‘wet signed’ copies, there is no need to store *both* hard copy and digital. Where hard copies *are* stored, IMPS recommend that these are secured behind ‘two barriers’, for example, a locked cabinet 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 ensure 'blind copy' methods of communication are used. Mistakes in this area, exposing 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.

'Anonymous' data

In data protection terms, 'anonymous' data is a very high bar. Truly anonymous data, 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 pseudonymised, not 'anonymous';
- 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 that researchers take care when using phrases such as 'your data will be anonymous', 'your data will be held anonymously', 'we will email you with a survey that will be anonymous' and similar. Instead, we would encourage researchers to use phrasing such as 'your data/information will be held in strict confidence', or 'your data will be held securely with access limited to those involved in the project'.

It is more useful to describe in layman's terms how the personal data will be handled, for example:

- 'The data you provide will be assigned a unique number and this data will be held separately from your identifying data, such as your name'
- 'The results of the study will be published in anonymous form and will not contain any data that will identify you'

Note: there is not a legal requirement *under data protection law* to advise participants of who may access truly anonymous data (as it not covered by the law itself). But researchers may wish to advise participants of this if they deem it appropriate or if it is required/courteous for reasons unconnected to data protection.

Data preservation and sharing

The University's Research Data Management Policy requires researchers to preserve primary data collected in support of project findings, and to make them accessible to others by deposit in a suitable public data repository, unless there is a valid legal, ethical or commercial reason for withholding access to them. The University provides guidance on choosing a data repository.

Most research data collected from research participants can be publicly shared *once they have been anonymised*, and data that are not suitable for public sharing can in most cases be shared on a controlled basis. It is not acceptable for applicants simply to state that research data cannot be shared for confidential reasons. If a researcher does not intend to share data they must explain and justify why the data are not suitable for sharing.

In order for publicly-disclosed data to be anonymised, any means of linking them to participant records stored internally should be removed, e.g. by replacing pseudonymous key codes linked to participant details with random identifiers.

Where data cannot be rendered safe for public sharing (for example, where identifying information is intrinsic to the data and cannot be removed), it may still be possible to share them with authorised users on a restricted basis. Some data repositories provide controlled access procedures for managing safe access to confidential or high-risk research data under a data sharing agreement or special licence. The University's Research Data Archive can accept and manage access to restricted datasets (including datasets containing identifiable information). The UK Data Service ReShare repository can accept and manage access to higher-risk anonymised datasets deposited as 'safeguarded' data.

Consent is not required to share anonymised data, although as a matter of good practice research participants should always be informed of plans to make any data collected from them available to others.

It is possible within data protection law to maintain and provide access to identifiable research data on an ongoing basis for 'archiving purposes in the public interest' and for 'scientific or historical research purposes', *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

The following can be contacted for advice on *specific questions or concerns* raised by the application, as relevant. Referrals should be made *by exception* and should be as specific as possible, with accurate reference to the relevant parts of the application. We have limited capacity to support School REC processes and will not review applications in full unless there is a need for doing so.

- **IMPS** (data protection): imps@reading.ac.uk / 0118 378 8981
- **Research Data Manager** (data management, preservation and sharing): r.m.darby@reading.ac.uk / researchdata@reading.ac.uk / 0118 378 6161
- **UREC** (research ethics): urec@reading.ac.uk

DMP assessment checklist

A Word version of this checklist is provided for download here.

☐ The required Data Protection information has been included in the participant information sheet (this could be presented in various ways, and language tailored or simplified to suit the audience, as long as it is covered).

☐ The researcher has considered how data will be securely stored and transferred during the project, and where relevant has been advised of risks and requirements (e.g. avoiding storage on external devices except where necessary, using encryption).

☐ Where references to 'anonymous' data have been made, these are deemed appropriate OR advice has been given to the researcher in relation to this.

☐ The researcher has considered how personal data required for long term retention will be managed and protected (for example if they leave the University).

☐ The consent form establishes the appropriate lawful basis for the processing of the personal data (usually 'public task') and does not *seek consent* for the processing of data (as per the sample data protection information for participant information sheets).

☐ If the researcher intends to ask recipients if they would be happy to be contacted about further studies, this is included in the consent form as an 'opt in' question.

☐ The consent form includes an 'I understand' statement regarding how their data will be used as described in the information sheet.

☐ The participant information sheet and consent form provide relevant information about the proposed preservation and sharing of research data (in most cases anonymised).

☐ The researcher has identified research data that will be preserved and made accessible to others on completion of the project or has justified why sharing of data will not take place.

☐ The researcher has identified a data repository that will be used to preserve and share research data (either openly or subject to controls) or has explained why such a solution is not suitable.

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

Sets out the University's requirement for the preservation and sharing of research data that substantiate published research outputs.