Guidance for Researchers

Forms A and B: Additional Guidance on Data Management

Re-use of Data

If you are applying for, or in receipt of, grant funding your funder may require that you make your data available to other researchers. There are mechanisms for doing this in a controlled environment and the research services team at the LLC (discovery@dundee.ac.uk) can advise on the options available to you. The future re-use of your data will not be possible unless you have fully informed participants in a way that is transparent and easily understood, and gained their consent.

Data re-use refers to the possibility of datasets being used for purposes for which they were not originally designed. This is allowed under data protection legislation where appropriate safeguards are in place (appropriate safeguards might include data minimisation and pseudonymisation). Participants need to be made aware that future uses of data may not reflect the current research question and so have to be given the option to opt in to this particular aspect of consent.

Following the end of the project participants will need to be informed of the storage location of their data and furnished with contact details for the repository/data controller in question. If your project data is to be stored in the University repository contact details are discovery@dundee.ac.uk.

The following is an example of text that can be used to obtain informed consent from participants for future use and re-use of the information by others along with some additional guidance notes on the information you will need to provide the participants so that they can make an informed decision:

“I give permission for the [specify the data] that I provide to be deposited in [name of data repository] so it can be used for future research and learning.”

Specify in which form the data will be deposited, e.g. de-identified (anonymised) transcripts, audio recording, survey database, etc.; and if needed repeat the statement for each form of data you plan to deposit.

Specify whether deposited data will be de-identified (anonymised), and how. Make sure to describe this in detail in the information sheet.

Specify whether use or access restrictions will apply to the data in future, e.g. exclude commercial use, apply safeguarded access, etc.; and discuss these restrictions with the repository in advance.

Taken from: https://www.ukdataservice.ac.uk/manage-data/legal-ethical/consent-data-sharing/consent-forms.

For further information on consent and example templates see: https://www.ukdataservice.ac.uk/manage-data/legal-ethical/consent-data-sharing/consent-forms.
Data Management Plan

Data management planning is the process of planning, describing and communicating the activities carried out during the research lifecycle. It is necessary to keep data safe, maximise data’s re-use potential and support longer-term preservation. It is considered good research practice and is now a requirement for many funding applications. The LLC has a guide on how to create a Data Management Plan on their web pages. Where personal data and special category personal data are collected for research, processing of data must be well documented in line with General Data Protection Regulation (GDPR). This would include keeping a record of:

- all correspondence with participants including consent
- safeguards in place to protect personal data

There is a freely available online tool that can be used for generating a data management plan which is approved by the University and major funders. The tool includes funder specific templates and advice - https://dmponline.dcc.ac.uk/.

You may need advice on how to safely collect, store, back-up and preserve your data. University of Dundee IT has policies and guidelines on the acceptable use of personal computing devices, mobile computing, remote access and encryption requirements.

**Data collected outside the UK**
Researchers collecting data abroad or in collaboration with international partners should make themselves aware of local legal requirements. It may be necessary to have a data sharing agreement in place with overseas partners to address the movement of personal data across borders.

**Data transferred outside the UK**
Similarly, personal data shared with partners overseas are subject to GDPR and may require a data sharing agreement. Data sharing/processing agreements are maintained by Legal.

See the University’s Data Protection advice on Data sharing/processing agreements for further information or contact dataprotection@dundee.ac.uk. If further information is required on other data management issues contact the research services team at discovery@dundee.ac.uk for assistance.

Additional information on conducting international research can be found at The Research Ethics Guidebook website: http://www.ethicsguidebook.ac.uk/International-research-104.

---

1 Special category data are sensitive personal data belonging to the following categories: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetics, biometrics; health; sex life; or sexual orientation.
Secondary Data

Secondary data that are already publicly available, for example, from social networking services, may have been collected and made available using consent processes based on a lower ethical standard than that usually applied to research. At the time of gaining consent, the new use of data for research purposes is not likely to have been anticipated. Research based on secondary data should therefore consider the possibility of harm to the data subjects.

Social networking services provide their users with a mechanism for withdrawing their data at any time, a service which is not easily replicated by researchers/research data repositories as there is no direct link to the data subject. As such it may be necessary to control access to data created by the research process, in some circumstances even after anonymisation, to protect the interests of data subjects.

It should be noted that whilst the purpose limitation principle of the GDPR requires that personal data are not further processed in a manner incompatible with the initial purpose for which data were collected, this does not necessarily preclude further research. Further advice should be taken from the University Data Protection Officer.

Re-identification

The effectiveness of anonymisation should be re-examined when datasets are looked at in relation to other publicly available data. There may be situations where “The removal of direct identifiers can no longer provide any confidence that the identity of the data subject is protected.”2 In such situations it may be necessary to consider providing controlled access to data; this will need to be costed in grant funding applications.

In cases where Funder requirements require that sensitive data be retained, University guidance is available from the research support team at the LLC (discovery@dundee.ac.uk) on services available to researchers for the safe storage, potential controlled access and long term preservation of data.

---

Data Storage: Location and Duration

The [University Policy to Govern the Management of Research Data](https://www.dundeecollegedocs.com) states that the length of time data is stored for should be determined as part of the research data management planning for the project, and should adhere to any particular funding body’s requirements and any additional conditions or practices within the field. Note that where there is an associated publication, data may need to be retained for verification of research findings.

Advice on how to safely collect, store, back up and share access to your data during a project, and subsequently store data for the longer term at the end of a project period, can be obtained from the research support team at the LLC ([discovery@dundee.ac.uk](mailto:discovery@dundee.ac.uk)).

The GDPR states:

‘You can keep personal data indefinitely if you are holding it only for:

- archiving purposes in the public interest;
- scientific or historical research purposes; or
- statistical purposes.

Although the general rule is that you cannot hold personal data indefinitely ‘just in case’ it might be useful in future, there is an inbuilt exception if you are keeping it for these archiving, research or statistical purposes.

You must have appropriate safeguards in place to protect individuals. When using special category data the following safeguards should be in place:

- technical and organisational security measures must be in place to ensure the security and integrity of the data. These measures should be documented. Technical security includes things like physical security, encryption and access controls. Organisational measures include things like research contracts and associated data sharing/processing agreements and research data management plans;
- the minimum amount of special category personal data must be used to achieve the aims of the research. You must be able to evidence that your research only uses the minimum amount of personal data and special category personal data;
- where you are able to work with anonymised data you must do so;
- where you cannot use anonymised data, you must use pseudonymised data if you are able. You should keep evidence of why you are unable to work with anonymous data;
- the use of identifiable data should be the last resort rather than a preferred option. If you are unable to use pseudonymised data you should keep evidence of why that was the case;
- if you are working with identifiable or pseudonymised data, you must move to anonymised data as soon as you are able;
• your research must not cause any individual substantial damage (normally actual or financial harm);

• your research must not cause any individual substantial distress (normally emotional or mental anguish or harm);

• you may not process data in your research to make decisions or take measures in relation to any individual unless you are working in ethically-approved medical research;

• you may not identify any individual in the results or statistical outputs of your research. Please keep this in mind when reviewing datasets for release as open data as well as in the production of reports, papers, briefings etc.