

Arts and Humanities Research Council (AHRC) Data Management Plan

1 Data summary

Briefly introduce the types of data the research will create. Why did you decide to use these data types?

AHRC guidance

When defining data types, consider the format/quality of the data and how you will make it as easy as possible to access the data.

Consult with your institution's data support (eg library services, IT department).

TUoS/DCC guidance: Data description

List the different types or categories of data you will be using, including physical samples and paper records. These may include experimental and survey data, as well as software and audiovisual data. Also indicate which data will be of long-term value and will therefore be preserved and/or shared.

Include any existing data or methods you will be reusing in your research. Describe how it will be used alongside your own data and how issues such as copyright and intellectual property rights will be approached.

2 Data collection

Give details on the proposed methodologies that will be used to create the data. Advise how the project team selected will be suitable for the data/digital aspects of the work, including details of how the institution's data support teams may need to support the project.

TUoS/DCC guidance: Data collection

Describe how you will collect and organise data to make them easier to find, understand and reuse. Explain how you will maintain consistency and quality. This is particularly important if data are generated by other people or a variety of equipment. Strategies may include using relevant standards, and processes such as calibration, repeat sampling and data entry validation.

Good practices when collecting and organising data include using version control, naming conventions, folder structure, peer review and controlled vocabularies.

See [Organising data](#) (TUoS) and [Data quality assurance](#) (UK Data Service).

3 Short-term data storage

How will the data be stored in the short term?

AHRC guidance

You should consult with the institution's data support (eg library services, IT department).

By submitting the DMP you are confirming that:

- The institution is able to store the data appropriately during the lifecycle of the grant, the relevant people have been consulted and this has been considered and agreed.
- The institution has considered all the risks, and storage will be in line with the institution's data management policy (provide a link to the policy if applicable).

TUoS/DCC guidance: Storage and security

Describe where each type of data will be stored and backed up during your research. Also identify who is responsible for managing your storage and backups, and how often backups will be carried out.

Storing data on laptops, computer hard drives or external storage devices alone is not recommended. Data and definitive project documentation should be stored throughout the project on centrally provisioned University of Sheffield [research data storage](#), which has automatic backup. Research groups are allocated up to 10TB free storage, which can be requested through IT Services. Further storage can be requested but may incur costs.

If any of your data are personally, commercially or politically sensitive, outline the main risks and how they will be managed.

Note any institutional data security policies that apply to the data. The University of Sheffield has policies relating to [information security](#) requiring its users to adhere, as a minimum, to the following security standards: [Information Security Policy](#); [GDPR and data protection](#). More secure system policies may be defined where necessary, for example where patient data is involved. University departments may have established their own policies regarding information security, eg [SchARR Information Governance Policy](#).

Please see the University of Sheffield webpage on [data security](#). See also [data storage guidance](#) from UK Data Service.

All University of Sheffield staff and researchers must complete online [information security training](#). If you require assistance, please contact the University's [Information Security Team](#).

Identify any formal data security standards with which you will comply. Please note that the University of Sheffield is not an accredited [ISO 27001](#) institution. The University provides email, contacts and calendaring services, Google Drive and Google Sites through the Google Apps for Education suite. Google Apps for Education (and the data centres that support the service) are SSAE 16 / ISAE 3402 Type II SOC 2 audited and have achieved ISO 27001 certification. The University is satisfied that personal data is being processed appropriately in accordance with UK Data Protection Law and the University's own privacy policies, and that the security controls put in place by Google are [sufficient to protect University data](#).

See the DCC Briefing Paper on Information Security Management ([ISO 27000](#)) and UK Data Service guidance on [data security](#).

Example text for high-risk data: "We recognise that this data is highly confidential and is critical to the clinical treatment of patients. Therefore a project-specific security policy has been developed in conjunction with the University's Information Security Team [link to policy]".

Suggested text for low-risk data: "The data will not include personal data relating to human participants. The University's [Information Security Policies](#) will be abided by at all times."

3a What backup will you have in the in-project period to ensure no data is lost?

See TUoS/DCC guidance: [Storage and Security](#)

4 Long-term data storage

How will the data be stored in the long term?

AHRC guidance

For advice on data storage and sharing, including future planning for the data, see:

[Digital Preservation Coalition Knowledge Base](#)
[Digital Curation Centre](#)

TUoS/DCC guidance: Preservation

Describe how you will preserve and share your data, including the length of time they will be kept and the nature of the storage location. Also indicate if any additional resources or funding will be required to deposit and store the data.

[UKRI](#) funders generally expect data with long-term value to be preserved and remain accessible, alongside the software and code needed to reproduce your findings. This does not mean that you need to keep all of your data, but you will need to state who will be responsible for choosing and archiving data, as well as documenting the removal of any data that must be destroyed. It is particularly important to preserve data which cannot be remeasured or recreated, such as earth observations or people-based data. See [Preserving data](#) for guidance on data selection and the [NERC data value checklist](#) for guidance on determining long-term value.

Many research funders specify which data need to be preserved, how long for and where they should be deposited. See University of Sheffield information on [research funder policy summaries](#), [research data repositories](#) and [making data discoverable](#). See also DCC guide [How to appraise and select research data for curation](#).

4a Where have you decided to store it, why is this appropriate?

TUoS/DCC guidance: Data repository

Long-term preservation and access is generally best managed by using a specialist repository. While you don't have to specify the repository you will use, you should state the criteria you will use to select it. When considering a repository, you should examine their policies, procedures, metadata standards and any costs that might be incurred. If using a storage facility other than an established repository or data centre, you will need to demonstrate its efficacy and longevity.

Some funders specify a data repository, such as [UK Data Service ReShare](#), [NERC Data Centres](#) or [Archaeology Data Service](#). Resources such as [re3data](#) and those provided by [BBSRC](#) or [Nature](#) can be used to find an appropriate repository. Some publishers, such as [PLOS](#), also provide lists of recommendations. University of Sheffield researchers can deposit data in [ORDA](#), the University's data repository; all research data selected for long-term preservation should be registered in ORDA, irrespective of where the data files themselves are deposited. Research data in non-digital formats, and digital data that cannot be made accessible or requires controlled access, should also be registered in ORDA.

See also [Making data discoverable](#) and [Research data repositories](#).

4b How long will it be stored for and why?

See TUoS/DCC guidance: [Preservation](#)

4c Costs of storage – why are these appropriate? Costs related to long-term storage will be permitted providing these are fully justified and relate to the project. Full justification must be provided in Justification of Resources (JoR).

AHRC guidance

Costs of preserving the data: See [4C \(Collaboration to Clarify the Costs of Curation\)](#)

TUoS/DCC guidance: Budget

Outline and justify resource costs involved in implementing the data management plan. These may include costs of storage, staff, data preparation or repository charges. Any support, training or technical assistance required to deliver the plan should also be noted.

University of Sheffield research groups can request up to 10TB free data storage during the lifetime of a project. There may be charges for larger or longer-term storage. Contact [IT Services](#) to discuss your requirements or obtain a quote.

The University of Sheffield research data repository, [ORDA](#), is free to use. You should enquire about charges made by other data repositories. If data are to be deposited anywhere other than an established data centre or repository, you should give details of how the data will be preserved and shared, including associated costs.

See UK Data Service guidance on [costing data management](#).

5 Data sharing

How the data will be shared and the value it will have to others

TUoS/DCC guidance: Data sharing

Outline which data you will share and how you will share them, eg depositing in a repository, using a secure data service or dealing with data requests individually. The method(s) used will depend upon the size and nature of the data. You should use standards and formats that enable reuse, and ensure data is discoverable through use of accurate metadata and persistent identifiers.

The Digital Curation Centre provides useful advice about [data appraisal and selection](#) and the [NERC data value checklist](#) provides guidance on determining long-term value.

Most funders allow a delayed release to allow researchers to have exclusive use of their data and to exploit the results of their research. See [Research funder policy summaries](#) to determine when you need to make your data available. Restrictions on the release of data may be allowed, to protect confidentiality and for other ethical and legal reasons. See [University and legal requirements](#) and UK Data Service [Legal and ethical issues](#) for more information.

While restrictions on sharing should be minimised, you should take into account the following when sharing data:

- Does your data include confidential and sensitive information?
- Have participants given consent for their data to be shared?
- Consider what can be done to make sensitive data openly sharable - can these data be anonymised?
- Do different parts of your data require different access conditions? These may require separate deposits.
- Who will be responsible for controlling access?

Access to and use of sensitive and confidential data can be restricted and regulated using [end user licences](#) or [data sharing agreements](#), or by using data enclaves. Whatever form of publishing is used, research data should be licensed to indicate what users may or may not do with the data. Data repositories will indicate what licences are available for the data they house. More information is available from the Digital Curation Centre on [how to license research data](#).

For all University of Sheffield research, a metadata record should be [registered in ORDA](#), the University's data repository. See also [Research data repositories](#).

5a How the data will enhance the area and how it could be used in the future

5b Releasing the data – advise when you will be releasing and justify if not releasing in line with AHRC guidelines of a minimum of three years. If the data will have value to different audiences, how will these groups be informed?

See TUoS/DCC guidance: [Data sharing](#)

5c Will the data need to be updated? Include future plans for updating if this is the case.

5d Will the data be open or will you charge for it? Justify if charging to access the data.

5e Financial requirements of sharing – include full justification in the JoR

See TUoS/DCC guidance: [Data sharing](#) and [Budget](#)

6 Ethical and legal considerations

6a Any legal and ethical considerations of collecting the data

AHRC guidance

By submitting the DMP you are confirming that:

- You have considered the legal considerations of collecting and releasing the data and have consulted with appropriate support.
- The data collection, creation, storage and dissemination will conform to the institution's ethical policy.

TUoS/DCC guidance: Ethics and privacy

Outline how you will handle any personal, sensitive or confidential data you will be using. Ensure all intended uses of the data are included explicitly in your consent form and ethics approval. This needs to cover secure storage, transfer, preservation and data sharing.

Describe measures you will take to protect the identity of participants, such as anonymisation or managed access procedures, which may avoid the need to delete data.

For guidance on ethical and legal issues, including GDPR, see [University and legal requirements](#) and UK Data Service [Legal and ethical issues](#). See also ICPSR's guidance on [data confidentiality](#) and [HIPAA regulations for health research](#).

6b Legal and ethical considerations around releasing and storing the data – anonymity of any participants, following promises made to participants

AHRC guidance

Consult with the relevant people in your organisation to ensure you are aware of any IP considerations and data protection requirements.

TUoS/DCC guidance: Intellectual property rights

State who will own the copyright and intellectual property rights of new and existing data, and how this may impact upon data sharing.

The University owns the data that you generate in the course of your research. In most cases you will still be able to use it for any research purpose. If you have collaborators or funders, you need to check agreements to see if they alter the rights to use of the data. If any data is involved in a patent application, you must not share it until you have consulted [Research Services](#).

You should apply a licence to any data you share, informing users how the data may be used.

Useful guidance can be found at:

- [University and legal requirements](#) (TUoS)
- [How to license research data](#) (DCC)
- [Rights relating to research data](#) and [Copyright \(licensing\)](#) (UK Data Service)
- [Data and software licensing wizard](#) (EUDAT)