



Data Management

Guidance for Grant Holders

Research data can comprise any supporting material which underpins or otherwise enriches the (written) outputs of research, including both quantitative and qualitative data. Research data can include, for example, audio recordings or transcriptions of interviews, spreadsheets with survey data, artwork produced by research participants, or photos and videos of research settings and activities.

Important principles that underpin Data Management include:

- **Transparency:** The evidence that underpins research can be made open for anyone to scrutinise, verify, and attempt to replicate findings.
- **Efficiency:** Data collection can be funded once, and data used many times for a variety of purposes. Much research data – even sensitive data – can be shared ethically and legally if researchers employ strategies of informed consent, anonymisation and controlling access to data.
- **Risk Management:** A pro-active approach to data management reduces the risk of inappropriate disclosure of sensitive data, whether commercial or personal. Security of data is especially important for research involving human participants.
- **Preservation:** Lots of data is unique and can only be captured once. If lost, it cannot be replaced.

Data often have a longer lifespan than the research project that creates them. Well organised, well documented, preserved, and shared data are invaluable to advance scientific inquiry and to increase opportunities for learning and innovation.

Each *Creating Safer Space* project is required to submit a Data Management Plan at application stage. Some grants are conditional on producing an improved Data Management Plan at the start of the project. This document provides guidance on how to answer each of the questions on the Data Management Plan.

This guidance is drawn from a variety of sources, including [Aberystwyth University, UK Research and Innovation](#), the [Digital Curation Centre](#) and [Protection International](#). There is further guidance about sources of information at the bottom of this document.

1. What types of data will the research collect or generate, and why have you decided to use these data types?

Research data can comprise any supporting material which underpins or otherwise enriches the (written) outputs of research, including both quantitative and qualitative data. Common forms of research data include, but are not limited to:

- Audio recordings or transcriptions of interviews or focus groups
- Surveys or spreadsheets with survey data
- Artwork or photos produced by research participants
- Photos or videos of research settings and activities
- Notes of participant observation, or fieldwork diaries
- Photos of archival material

Explain what research data your project will use, and if the data will be generated by your own project, or whether you will use existing or third-party sources of data (e.g. survey data produced by another project).

Think carefully about whether there is existing data available that could be re-used, before proposing to collect or generate new research data. [DataCite](#) has a search engine for their global dataset catalogue.

Explain why you have decided to collect or generate your selected forms of research data, and specify the format of the data (e.g. whether it will be hardcopy or electronic, and what file format or software will be used).

2. What methodologies will be used to create the data? What experience or knowledge does the project team have about this aspect of the work, and will the Lead Organisation's data support team provide additional support to the project?

Explain the methodologies that will be used to create each of the data types described above. For example, if you are using interviews, explain how the interviews will be recorded (audio and/or notes) and whether/how/when you will transcribe the interviews. Describe how you will ensure consistency and quality of data, how you will structure and name your folders and files and how you will handle version control (see the [Aberystwyth University guidance on Organising your Data](#)), if/how data will be shared between collaborating organisations, and how you will anonymise data, if applicable (see the [Creating Safer Space guidance on Research Ethics](#)).

Explain what experience or knowledge the project team has about this aspect of the work. Have you generated similar types of research data in a previous project, or have you undertaken specific training on this aspect of the work? Allocate clear roles and responsibilities for all data management aspects, and ensure the people to undertake the roles have relevant expertise or will receive appropriate training.

Explain whether the Lead Organisation's data support team will provide additional support to the project.

3. How will the data be stored in the short term? What backup will you have during the project to ensure no data is lost? How will data be protected?

Describe how the data will be stored in the short term (for the duration of the project). Consider whether you have sufficient storage capacity for all the data that your project will generate.

Describe how often data will be backed up, and to which locations, to protect against loss. In devising your plans, think about the various ways in which research data could be lost (e.g. through computer malfunction, a fire, a lost suitcase or theft) and how to mitigate against such loss. Describe who will be responsible for backup and recovery, or any automated backup services that will be used (e.g. [rsync](#)).

Describe how data will be protected against unauthorised access (both in the main locations and in the backup locations). Please see below for some advice on common methods of protecting physical and digital data, respectively.

Common methods of protecting physical data	
What to do	How to do it
Store physical material in securely locked rooms and/or filing cabinets, and control access.	Ensure storage is securely locked, and that only a small number of authorised individuals have access to a key or code. Log who has access to such storage locations, and log any removal of material.
Minimise the collection or retention of sensitive physical data that cannot be stored in securely locked facilities.	If you are undertaking fieldwork in a location which lacks secure facilities for storage, consider whether fieldwork diaries or notes can be transcribed and safely uploaded to a secure online location at regular intervals, instead of being retained in physical format. If this is not possible, assess the security implications of the data being lost, stolen, or inspected by local individuals or authorities.
Securely dispose of physical data that is no longer needed.	Use a shredder or equivalent to destroy physical data that is no longer needed.
Send sensitive physical data to collaborators or others (e.g. transcribers) through secure means.	Ordinary post is usually not secure. Use tamper-proof/evident postal packets. Recorded delivery is a secure method of sending sensitive physical data to collaborators in some countries, but not all. Digitisation and secure web transfer is preferable.

Common methods of protecting digital data

What to do	How to do it
Ensure the safety of any computer where sensitive digital data is stored.	Encrypt your computer and/or storage (e.g. Bitlocker or VeraCrypt); use a strong password to protect your computer; install a firewall system; install anti-virus software; receive security-related upgrades to your operating system.
Ensure the safety of any digital storage devices.	USB drives and external hard drives should be encrypted (e.g. Bitlocker or VeraCrypt). Their use should be avoided where possible.
Avoid transport of data across borders.	Sensitive data is best stored encrypted on institutional systems and not on devices which could be inspected by authorities when travelling (such as the US, where researchers can be compelled to unlock any encrypted data and turn over encryption keys).
Minimise sending sensitive data files to collaborators.	Consider carefully whether you need to send sensitive data to collaborators. For example, do you really need to send the audio recordings of the interviews, or would it be sufficient to send the anonymised transcripts?
Communicate with and send sensitive digital data to collaborators or others (e.g. transcribers) through secure means.	<p>To send data digitally, consult your institution's Data Security team for advice on secure ways to send data. They may have contracts with third party providers, that they have assessed to be safe. Carefully assess the security systems of any third-party providers, as well as the legal jurisdiction in which the data is held.</p> <p>Email is usually not a safe method of sharing sensitive data. Encrypt documents before sending them through email. The UK Data Archive gives GnuPG as an example of reliable open source encryption software. Aberystwyth University recommends VeraCrypt as an alternative option. The password to the VeraCrypt container will need to be separately and securely communicated to the recipient.</p> <p>Phone SMS is not a safe method of sharing sensitive data.</p> <p>Protection International recommended Signal, Jit.si (note that the location of Jit.si server is important), Share Riseup and</p>

	<p>chApril in June 2021 as comparatively safe methods of communication and data sharing, but this may have changed since then – please do some research into any third party providers used.</p> <p>Insecure methods of online sharing are often thought to include WhatsApp, MS Teams, Skype, Zoom, Facebook, DropBox, YouSendIt. Protection International advise that Google and Apple are good on security, but data is not protected very well by US Privacy Laws. If you use any of these providers, assess the security implications carefully.</p>
Securely dispose of digital data	The UK Data Archive provides guidance on how to securely dispose of digital data (p. 21).

For both physical and digital data, describe any legal agreements that will be in place for sharing data. Confidentiality or data sharing agreements may be required before sharing sensitive data with collaborators or other third parties, such as transcribers or other researchers who are interested in the data. Ask people to securely dispose of the data, once they no longer need it, and follow up to ensure they remember to do it.

Carefully consider the level of protection required for each data type. Research data that is publicly available still needs to be protected against loss, but unauthorised access may be less of a concern, and you may be able to share the data with your collaborators by unencrypted email. In contrast, a high level of protection is required for sensitive personal data and for confidential information. Think carefully about whether you can use anonymisation to mitigate the negative consequences of unauthorised access (see the Creating Safer Space guidance on [Research Ethics](#)).

4. How will the data be stored in the long term, and why is this appropriate? How long will it be stored for and why?

Describe how data will be stored in the long term (after the conclusion of the project), and why this is appropriate (bearing in mind the security considerations described above). If any data will be deleted at the end of the project, explain why.

Consider whether research data can be safely stored in a national or international data service or subject-specific repository, such as:

- [UK Data Service](#): This repository stores and shares primary research data from the social and behavioural sciences.
- [Zenodo](#): This repository stores and shares primary research data from across the world. The repository is hosted by CERN (the European organisation for nuclear research), but it accepts research data from across all disciplines.
- [Mendelay Data](#): This repository stores and shares primary research data from across the world, in all disciplines. The repository is owned by Elsevier, but it is free to use.

Digital research data collected as part of *Creating Safer Space* projects can normally be stored at Aberystwyth University after the end of the project for a period of up to 10 years. The data can be stored with restricted or open access. Please contact us at an early stage if you would like to enquire about this possibility, and please consider whether your Participant Consent Forms need to be written in such a way as to enable the transfer of data to Aberystwyth.

Describe what file formats you will use for long-term storage. Initial file format may be determined by the specialist software used to create or collate data, but for the data to be used in the long-term or shared, it may need to be converted to a more widely used format (see [UK Data Service guidance on recommended file formats](#)).

Describe how long data will be stored for and why. UK Research and Innovation (UKRI), the funder of the *Creating Safer Space* network, suggests data that by their nature cannot be recreated (such as data from interviews) may often warrant indefinite storage and preservation. On the other hand, UKRI also recognizes that it may not be possible or cost-effective to preserve research data: this will depend on the type and scale of the data, their role in validating published results, and their predicted long-term usefulness for further research. UKRI expects data that underpins findings in publications to be accessible for at least ten years after publication.

Please ensure you have considered how to pay for any costs associated with long-term data storage.

5. Will the data be shared, and if so, how? What value does the data have to others, and how could it be used in the future? When will you release the data? If the data will have value to different audiences, how will these groups be informed? Will the data need to be updated, and if so, what are your future plans for doing this? Will the data be open, or will it be made available upon request?

UK Research and Innovation (UKRI), our funder, expects research data to be shared and openly accessible to other researchers without a charge. Publicly funded research data are a public good and produced in the public interest, and should be made openly available with as few restrictions as possible in a timely and responsible manner.

Exceptions can be made where there are good reasons not to share data openly. We appreciate that some *Creating Safer Space* projects will have good reasons not to share data openly, given the security contexts of the regions in which our projects take place and the difficulty of fully anonymising data derived from qualitative research with small groups or communities. If the research data cannot be shared, present a strong case for why not. The other questions in this section are then not applicable.

If the research data will be shared, describe how. Will it be deposited in your own organisation's institutional repository, and does this have specific mechanisms for public access? Will it be deposited in an external repository, and if so, is this repository open to all disciplines or a discipline-specific repository? Is it free to use and access? As a last resort, would the research team handle requests for access to research data directly?

Describe what contextual information you will provide to enable other researchers to understand the data, in order to minimise unintentional misuse or misinterpretation of the data. For example, this can include information about who created or contributed to the data, when the data was collected, the methods used to collect the data, information about how

the data has been processed and managed, and details about how the data is labelled and organised.

Describe what value the research data will have to others, and how it could be used in the future. Might other researchers wish to use the data to validate your research findings, to conduct new studies, or for teaching?

Explain when you will release the data. This should be as soon as possible after the grant ending, but UKRI recognises that grant holders may be entitled to a limited period of privileged use of the data they have collected, to enable them to publish the results of their research. Data should normally be released no later than the publication of the main findings, and within three years of the grant ending.

Describe whether the data will have value to different audiences, and how these groups will be informed of the existence of the data. At a minimum UKRI expects all published research results to include information on how to access the supporting data. We also recommend including this information on your own organisation's website, and on your project page on the *Creating Safer Space* website.

Describe whether the data needs to be updated, and if so, what your future plans are for doing this, and how this will be financed.

Describe whether the data will be open, or whether it will be made available upon request. If the latter, what will be the conditions for approving any requests, and who will make the decision? For example, you may wish to consider concluding a data sharing agreement before sharing sensitive data.

6. Are there any legal and ethical considerations of collecting the data, or around releasing, sharing and storing the data (e.g. anonymity of participants)?

Describe any ethical considerations of collecting, releasing, sharing, and storing the data. How will you anonymise personal data, before sharing? How will your Participant Consent Forms include permission to share research data, if applicable?

Describe any legal considerations of collecting, releasing, sharing, and storing the data, for example in regards to confidentiality or any applicable Data Protection Law. Will you need to conclude data sharing or non-disclosure agreements before sharing sensitive data?

Describe any intellectual property considerations of collecting, releasing, sharing, and storing the data. For example, if you share the data, what kind of licence will you use? Many projects choose to licence their data with a CC BY (attribution) licence, which means that if anyone reuses the data, they must give you appropriate credit.

See the [Creating Safer Space guidance on Research Ethics](#) and the [UK Data Archive guide to Managing and Sharing Data](#) (pp. 22-27) for further advice.

FURTHER INFORMATION

The Digital Curation Centre (DCC) offers a [How-To Guide to Developing a Data Management Plan](#), a [Checklist](#), and some [Data Management Plan examples](#).

UK Research and Information (UKRI) provides and [Guidance on Best Practice in the Management of Research Data](#)

The UK Data Archive provides a guide on [Managing and Sharing Data](#).

JISC provides a [toolkit](#) for Research Data Management.

JISC provides information about the [FAIR principles](#) of research data management, which are considered international best practice.