

Digit Data Manual

Version 2: April 2023

Contact: Prof Chris Forde, Digit Deputy Director & Digit
Data Observatory lead (cjf@lubs.leeds.ac.uk)

Table of Contents

OVERVIEW OF DIGIT DATA MANAGEMENT AND KEY REQUIREMENTS	4
KEY PRINCIPLES OF DATA MANAGEMENT IN DIGIT	4
ESTABLISHING A DATA MANAGEMENT PLAN FOR YOUR DIGIT RESEARCH	6
THE DATA YOU INTEND TO GATHER OR USE DURING THE PROJECT	6
METHODOLOGIES FOR DATA COLLECTION AND PROCESSING	6
ETHICAL AND LEGAL REQUIREMENTS.....	7
DATA STORAGE	7
DATA SHARING AND ARCHIVING	7
FURTHER RESOURCES ON ESTABLISHING A DATA MANAGEMENT PLAN	8
ETHICAL CONSIDERATIONS	9
ESRC & ETHICS.....	9
FURTHER GUIDANCE ON ETHICS	10
DATA PROTECTION	11
KEY ASPECTS OF DATA PROTECTION	11
ANONYMISING DATA	11
INFORMED CONSENT	12
FURTHER GUIDANCE ON DATA PROTECTION	13
STORING AND HANDLING DATA	14
TRANSCRIBING DATA	16
SHARING AND REUSING YOUR DATA	17
ARCHIVING YOUR DATA	18
PREPARING DATA FOR ARCHIVING: UK DATA SERVICE GUIDANCE.....	18
<i>Study level documentation</i>	18
PREPARING YOUR DATA FOR DEPOSIT: RESHARE GUIDANCE	20
<i>Open data (Creative Commons licences)</i>	21
<i>Safeguarded data</i>	21
<i>Controlled data</i>	21
FURTHER GUIDANCE ON PREPARING DATA FOR ARCHIVING	21
APPENDIX A: CHECKLIST OF UNIVERSITY POLICIES ON RESEARCH DATA AT THE UNIVERSITY OF LEEDS	22
APPENDIX B: CHECKLIST OF UNIVERSITY POLICIES ON RESEARCH DATA AT THE UNIVERSITY OF SUSSEX	23
RESEARCH DATA, PUBLICATIONS AND OTHER OUTPUTS	23
APPENDIX C: LINKS TO USEFUL RESOURCES AT UKDS, UKDA AND ESRC	25

Version control

Please, note, this is a live document subject to changes. Please check the version you are working on, and note the changes below.

Version	Date	Changes
Version 1	July 2021	Original
Version 2	April 2023	<p>Minor typographical edits throughout</p> <p>Updates to website link re: data access statement</p> <p>Clarification in a couple sections that Innovation Fund awardees must follow guidelines, e.g. who needs to follow Ethics procedures</p> <p>Storing & handling data: update to phase out date of M and N drives at Leeds</p> <p>Several edits to section Archiving your data: new first sentence; UKDS link added that shares a video explaining the ReShare process; new request for adding 'Digital Futures at Work Research Centre' as the Alternative Title when depositing data via ReShare</p> <p>Appendix B: minor edits attributing links to Sussex; new links that take in to account the updated Open Access rules from UKRI from 1 April 2022.</p>

Overview of Digit Data Management and Key Requirements

This data manual is designed to provide information and resources for anyone involved in generating, analysing, storing and archiving data as part of the ESRC Digital Futures at Work Research Centre (Digit). Digit has been funded by the ESRC from 2020-2024. It is led by Leeds University Business School and the University of Sussex Business School, with partners from Aberdeen, Cambridge, Manchester and Monash Universities¹.

The specific ways in which you will gather, use, analyse and store data as a researcher in Digit are likely to vary from project to project. However, there are some data management principles and practices that are common across the ESRC, the Universities of Leeds and Sussex, and the other institutions involved in Digit. In this data manual we look to synthesise the present core principles that you should comply with in your management of data. Specific links, where relevant, are made to guidance at resources at the Universities of Leeds, Sussex along with the ESRC and the UK Data Service (UKDS) and UKDS partner lead, UK Data Archive.²

Key principles of data management in Digit

- Generation and use of any data should comply with the specific requirements of the institution(s) where you are employed, as well as Digit (ESRC) and any other funders.
- Research projects should ensure that the capture, management, integrity, confidentiality, preservation, sharing and publication of research data comply with relevant institutional level ethical frameworks.
- Primary responsibility for the management of data during a project lies with Principal Investigators (PIs), but every member of research teams also has responsibilities for compliance.
- Your employing institution, the ESRC, and the UK Data Service all provide support, training and advice on the management of data. Please see the links to resources provided at the end of this document. At Digit, Chris Forde as Data Observatory lead can be contacted for advice at c.j.forde@lubs.leeds.ac.uk
- Data management plans should be put in place for each research project conducted as part of Digit.
- Digit has a commitment to the open sharing of research data, where this is permitted, and possible
- PIs, Lead investigators, Visiting Fellows and Innovation Fund grant holders (where applicable) should, where possible offer data for deposit and preservation in the UK

¹ <https://digit-research.org/>

² <https://esrc.ukri.org/funding/guidance-for-grant-holders/research-data-policy/>
<https://www.data-archive.ac.uk/managing-data/>
https://library.leeds.ac.uk/info/14062/research_data_management/61/research_data_management_explained
<http://www.sussex.ac.uk/library/researchdatamanagement/>

Data Service no later than 6 months after the end of a specific project within Digit (but no later than 31 March 2025).

- Data should be prepared for archiving in line with the guidance provided in this manual, and the Digit Centre Manager and Data Observatory Lead, Chris Forde, should be notified when any data are ready for archiving, also cc:ing digit@sussex.ac.uk.
- The funders of Digit, the ESRC, supports the position that most data can be curated and shared ethically provided researchers pay attention right from the planning stages of research to the following aspects:
 - when gaining informed consent, include consent for data sharing
 - where needed, protect participants' identities by anonymising data; and
 - address access restrictions to data in the data management and sharing plan, before commencing research.
- The ESRC regards non-deposit of research data as an exception. Waivers may be granted where researchers have demonstrated due diligence in all three areas. Where issues of confidentiality are foreseen that would prevent data being successfully shared, Digit researchers are encouraged to contact The Data Observatory lead, Chris Forde (ccing digit@sussex.ac.uk) and the relevant data service provider (currently the UK Data Service) at the earliest opportunity. In order to provide a waiver the UKDS will require the Data Management Plan and blank copies of consent forms and information sheets used; if you consider a waiver is necessary you can contact the UKDS at reshare@ukdataservice.ac.uk.
- Current ESRC guidelines around depositing and non-depositing of data can be found here: <https://esrc.ukri.org/files/about-us/policies-and-standards/esrc-research-data-policy/>
- The approach being adopted for archiving should be specified in the Data Management Plan
- Links to data produced as part of Digit that are archived at the UK Data Service (UKDS) will be listed on the UKDS website, and also on pages in the Digit Data Observatory. You are welcome to also list these on your own institution's website.
- Published papers which rely on data generated through Digit should include a data access statement. This statement indicates how and where others can access the data used in the paper. Guidance on writing a data access statement and some examples can be found here: https://library.leeds.ac.uk/info/14062/research_data_management/66/sharing_data/6. Published papers should include an acknowledgement to the ESRC and Digit (if you are not aware of the correct acknowledgement procedures, please email digit@sussex.ac.uk).

Establishing a Data Management Plan for your Digit research

For all Digit-funded research projects, we advise that you put in place a clear data management plan. This plan is useful to help you set out how you will gather, analyse, store, share, archive and destroy data. It is a requirement for all ESRC funded projects, and is typically outlined in basic terms in bids, and then developed before and during projects. Both the University of Leeds and Sussex, the lead partner institutions in Digit, offer detailed guidance on designing data management plans, as do the ESRC. The advice presented synthesises key points from this guidance. Links to more detailed guidance are available here:

- ESRC: <https://esrc.ukri.org/funding/guidance-for-grant-holders/research-data-policy/>
- UK Data Service: <https://www.ukdataservice.ac.uk/manage-data/plan/dmp-esrc/data-management-plan.aspx>
- University of Leeds: https://library.leeds.ac.uk/info/14062/research_data_management/62/data_management_planning
- University of Sussex: <https://www.sussex.ac.uk/library/researchdatamanagement/>

Your data management plan should set out the following:

1. The data you intend to gather or use during the project
2. Methodologies for data collection and processing
3. Ethical and legal requirements
4. Data storage
5. Data sharing and archiving

Further details of each are provided below.

The data you intend to gather or use during the project

The ESRC indicates that this should cover:

- data volume (how much data, from which sources)
- data type (primary, secondary; quantitative, qualitative;)
- data quality, formats, standards documentation and metadata (this information is useful to consider and set out at the start of the project, as it will ultimately inform and impact upon data archiving options at the end of the project – see Archiving your data below).

Methodologies for data collection and processing

- Here you should consider and set out the data collection methods you will use (surveys, interviews, case studies, ethnography, observation, focus groups etc).

- You should also specify the means through which you will capture data (recording interviews, collecting surveys electronically, observation with field notes etc).
- You should also give an indication of how you will access any secondary data (sources, how it will be transferred to you)

Ethical and legal requirements

- Your data management plan should set out whether there are any legal restrictions on accessing and using data, and also set out the steps you will take to ensure ethical requirements (at both an institutional and ESRC level) are met. These issues are considered in more detail in Section 3 below.
- You should also consider whether you will be looking to place any restrictions on access and use of data, both during and after the end of your project. These restrictions may be needed for a range of reasons – to comply with restrictions in place working with particular organisations or individuals, to maintain anonymity or confidentiality, to limit access to sensitive data, to address data where copyright is held by other parties. Access safeguards can be out in place for e.g. depositor permission or controlled access. Personal data (i.e. data that can identify individuals) should not be shared, and so steps should be taken to ensure data is anonymised before it is shared and archived. Further guidance here can be found in the UKDS's FAQs on Managing data: <https://www.ukdataservice.ac.uk/help/faq/manage-data.aspx#PeriodStored>
- You should consult and work with ethics, legal and data management specialists at your own institution to develop these parts of your data management plan. An ethical review, and possible application (depending on your institutions processes), will be necessary at your own institution before the commencement of any data collection on a Digit research project. In regards to consent covering data sharing, if in doubt, please consult the UK Data Service by email at datasharing@ukdataservice.ac.uk.

Data storage

It is important to consider how you will store data securely, both quantitative and qualitative, and being mindful of the format or software used for data storage, during and after the end of the project. Your individual institution will have specific preferences for storing data locally in a secure manner during the course of a project. For longer-term data archiving, we recommend that you deposit data in one archive, so that any amendments only need to be made in one repository. In this manual, we set out guidance from the ESRC and both the Universities of Leeds and Sussex.

Data sharing and archiving

Whilst data archiving typically takes place at the end of a project, you should consider this and put in place a plan for archiving at the start of the project where possible. Consider whether and how you want to share data with others, and how this might be done. Where possible and appropriate, we want all Digit data to be made available after the completion of

an individual project through the UK Data Service. Guidance on preparing data for archiving through the UKDS is provided in Archiving your data below.

[Further resources on establishing a data management plan](#)

There are some templates and examples available online to help you put together a Data Management Plan. There is a very useful DMP checklist on the UK Data Service website: <https://www.ukdataservice.ac.uk/manage-data/plan/checklist.aspx> that can help identify some of the best practises for data sharing and management The DMP Online Tool, provided by the Data Curation Centre (DCC) at the University of Edinburgh, is an online resource, recommended by the ESRC, to help you develop a Data Management Plan that complies with ESRC requirements. This tool is available here: [https://dmponline.dcc.ac.uk/about us](https://dmponline.dcc.ac.uk/about_us).

Sign up with your institutional accounts as this may automatically give access to additional guidance and support written by your institution. For example, at the University of Sussex, you can 'request feedback' and a member of the Library staff will review. You can also 'select guidance' from a variety of organisations to view and add to your DMP as you write it.

Please check in with your local institution to understand timescales for DMP reviews were offered, as they will vary.

A more detailed guide from the DCC on producing a data management plan can be found here: <https://www.dcc.ac.uk/guidance/how-guides/develop-data-plan>

Ethical considerations

All research conducted as part of Digit should comply with institutional ethical standards and also comply with any legal requirements.

ESRC guidance on ethics is that all ESRC-funded research should benefit from an appropriate ethics review, in order to ‘help researchers reach high standards, and to support and protect all the parties involved in research. Ethics scrutiny should assess the risks and benefits of a project, consider the balance between, and take a proportionate view of whether risks which cannot be eliminated may or may not be justified.’³

The ESRC does not prescribe the nature of ethical review to be undertaken, but instead recommends that it is the responsibility of the researcher – guided by standards set by their professional society, disciplinary body and employing institution, to determine the type of review that is required. **For Digit research, you should follow the ethical review process detailed by the employing organisation of the lead or principal investigator, visiting fellow or Innovation Fund grant holder (if appropriate) on any project. This is almost certainly likely to require an application to a University ethics committee prior to the commencement of the project.** If you are not a member of a University or research institute where there is an ethical review committee, please speak to Digit directly.

Ethical review within a University / research institution may involve a light touch review and/or full review. Light touch reviews may occur where projects can be identified that have a low risk to participants and any others affected by the research. Projects which involve more than minimal risk should receive a full ethics review.

ESRC & ethics

ESRC principles of ethics, which should be followed by all Digit research are as follows:⁴

- “All ESRC-funded research must be subject to an appropriate ethics review. Where the risk of substantive harm to participants (and others affected by the proposed research) is minimal, a light-touch review may be appropriate.
- An ethics review must be proportionate to the potential risk or harm that the research imposes. Risks should be balanced against benefits and, where possible, risks should be minimised. Ethical considerations are different where there is minimal risk of serious harm, and moderate risk of minimal harm. These considerations apply whether the research involves primary use as well as the re-use of data.
- Researchers are responsible for identifying potential ethics issues that may arise within a project and determine the appropriate type of review that is required, guided by their professional ethics codes and standards of the employing organisation. If only a light-touch review is required it must be fully justified. Research proposals involving human participants and personal data may require full review by the appropriate

³ <https://esrc.ukri.org/funding/guidance-for-applicants/research-ethics/>

⁴ <https://esrc.ukri.org/funding/guidance-for-applicants/research-ethics/our-core-principles/>

Research Ethics Committee which has been established and operates in accordance with the principles and guidelines set out in this framework.

- A single review process should be agreed in collaborative research involving more than one organisation or multidisciplinary research. The principal investigator should ensure that participating organisations and collaborative researchers are satisfied that the research proposal has received adequate ethics review, and that regular monitoring of the conduct of the research takes place and is promptly reported to all organisations and researchers involved.
- Freelance researchers, or institutions without their own procedures for independent review, must arrange for any ESRC-funded research to be submitted to an ethics review procedure.
- All data collection and analysis involving human participants or personal data should receive light-touch or full ethics review before the research commences.
- In the majority of cases, research proposals should be submitted for ethical review immediately after notification of funding, but it could also be prior to a pilot study so that participants' interests are protected; prior to seeking the agreement of potential research sites and gatekeepers so they can be assured of its good standing; or prior to the main data collection.
- As research progresses, further ethics issues may arise. Principal investigators should check through the implications of the issues and have these reviewed by the appropriate ethics committee. Non-conflicting advisory bodies, independent experts and mentors may also assist in this process.
- Approval for minor changes to a project following ethical review is delegated to the institutional level."

Further guidance on ethics

Guidance from the University of Leeds on ethical review and good practice in ethics can be found here: <https://ris.leeds.ac.uk/research-ethics-and-integrity/ethics-and-ethical-review/>

Guidance from the University of Sussex on ethical review can be found here: http://www.sussex.ac.uk/staff/research/governance/erp_overview

Increasingly, data are being gathered using video conferencing platforms, such as Zoom, Skype and Teams. Researchers should ensure that in collecting data via these means, they are following any institution specific guidance around the use of these platforms. Guidance from the University of Sussex, for example, can be found here: <https://www.bsms.ac.uk/pdf/research/the-use-of-video-conferencing-services-for-research-approved.pdf>.

Data Protection

Research conducted as part of Digit needs to comply with the Data Protection Principles embodied in the Data Protection Act 1998. Any use of personal data is seen as ‘personal data processing’. The main provisions of the act can be found here: <https://www.legislation.gov.uk/ukpga/1998/29/contents>

The ICO guide to data Protection can be found here: <https://ico.org.uk/for-organisations/guide-to-data-protection/>

ESRC guidance on Data Protection can be found here: <https://esrc.ukri.org/funding/guidance-for-applicants/research-ethics/frequently-raised-topics/data-requirements/data-protection/>

Key aspects of data protection

Key aspects of data protection that you need to consider are set out below. If you are answering yes to any of these questions, then you should address these issues, and explain how you will manage these data in an ethical review:

- **Am I using personal data?** – in other words, data which relate to a living individual who can be identified? This includes expressions of opinions about individuals, and indications of intention, as well as demographic and personal information.
- **Are any of the data sensitive personal data?** – this is defined in the Data Protection Act as data on: “a person's race, ethnic origin, political opinion, religious or similar beliefs, trade union membership, physical or mental health condition, sexual life, commission or alleged commission of an offence, proceedings for an offence (alleged to have been) committed, disposal of such proceedings or the sentence of any court in such proceedings”.
- **Are the data confidential?** – have you been provided access to data/information on agreement that this will be kept confidential, or is the information not in the public domain?

Anonymising data

You shouldn't disclose personal information that you hold as part of your research to others, unless consent has been explicitly given by a respondent/participant.

You should anonymise your data to ensure that individuals cannot be identified by third parties.

The UK Data Service has compiled a useful guide to anonymising your research data: <https://www.ukdataservice.ac.uk/manage-data/legal-ethical/anonymisation.aspx>. It has detailed information on anonymising both quantitative and qualitative data and a step-by-step guide. This guide advises anonymising your data by:

- removing direct identifiers, e.g. name or address
- reducing the precision of information or a variable, e.g. replacing date of birth by age groups

- generalising the meaning of detailed text, e.g. replacing a doctor's detailed area of medical expertise with an area of medical speciality
- using pseudonyms
- restricting the upper or lower ranges of a variable to hide outliers

This process can be time-consuming and you should consider the financial and time aspects of this in your data management plan.

Informed consent

For all Digit research projects, you are expected to obtain **informed consent** from those who participate in your research. Under informed consent, participants should be clearly made aware of the following:

- purpose of the research
- what is involved in participation
- how they can withdraw
- How the data will be used
- How data will be stored
- Whether the data will be archived and made available to others
- Whether and how data will be shared
- strategies to ensure confidentiality of data where this is relevant – anonymisation, access restrictions, etc.

You should seek to ensure that participants understand these aspects of the use of their data and should obtain written or verbal consent from participants once you are confident that they do understand. Inferring consent from non-response to a communication such as a letter is not appropriate.

For detailed interviews, or where personal, sensitive or confidential data are gathered, the ESRC, and Universities of Leeds and Sussex all advise the use of *written consent* forms to ensure compliance with the Data Protection Act, funder, and institutional guidance.

This will typically involve an information sheet and a consent form which will be signed by the participant.

For surveys or informal interviews, where no personal data are gathered or personal identifiers are removed from the data, obtaining written consent may not be required. However, it is still seen as good practice to obtain written consent from respondents through surveys, typically through the provision of a series of consent questions completed at the start of a questionnaire survey. In all cases, an information sheet should typically still be provided indicating the purpose of the research, how data will be used and the identity of the researcher(s).

Further guidance on data protection

Real research example consent forms covering different data collection methods and a consent form template recommended by UKDS can be found on the UK Data Service site:

<https://www.ukdataservice.ac.uk/manage-data/legal-ethical/consent-data-sharing/consent-forms.aspx>

Example information sheets and consent forms from the University of Leeds and University of Sussex can be found here:

- Leeds: <https://ris.leeds.ac.uk/research-ethics-and-integrity/other-resources/approaching-and-recruiting-research-participants/>
- Sussex: http://www.sussex.ac.uk/staff/research/governance/apply/ethics_a_z#consent

Storing and handling data

Your data management plan should indicate clearly how you will store and handle any data generated as part of a Digit research project, and this should be communicated to all researchers involved in the project.

Guidance on data storage varies from institution to institution. The following are broad principles which apply across institutions and are seen by the ESRC and the UK Data Service as good practice: you should follow these steps, and then look at the specific preferences and protocols for local and remote storage in your own institution. **Digit does not itself store primary or secondary project data – during the course of a project, you and other researchers working on a project should store this securely yourself.** After a project is completed, where possible, data will be archived in the UK Data Service and made available to the wider research community.⁵

Key advice to follow around data storage:

- Use managed and backed-up storage where possible – ideally storage provided by your faculty or central IT. Storing your data in managed and supported drives will help to reduce both the likelihood and scale of data loss that can occur.
- You can also use portable data (laptops, tablets, mobile phones, cameras, audio recorders) to record data. Portable data should be password protected and encrypted in line with your institutional policies. You should transfer this onto University storage as soon as possible.
- No sensitive data (as defined by the Data Protection Act) should be stored on laptops unless they are protected by appropriate encryption software. USB storage devices should also be encrypted where you are handling sensitive data files.
- Transfer data that you have generated in the field to managed storage as soon as possible.
- Ensure that you have data back-up procedures in place, including all institutions/collaborations on a project
- Develop shared folder and file naming conventions across the team
- Allocate responsibility for the immediate day-to-day management, storage and backup of research data. The default is that a principal investigator has overall responsibility.

At the University of Leeds, the recommended places for data storage are the cloud-based OneDrive and Teams/Sharepoint. OneDrive does allow sharing of files internally and externally to the university. OneDrive is good for storing individual work and for ad-hoc

⁵ Please note: *The UK Data Service* is funded by the UK Research and Innovation, through the Economic and Social Research Council to meet the data needs of researchers, students and teachers from all sectors. Based at the University of Essex, the *UK Data Archive* is the lead partner of the UK Data Service, providing researchers with support, training and access to the UK's largest collection of social, economic and population data. Both the UK Data Service and the UK Data Archive are a source of support and information, but data should actually be deposited to UK Data Service.

sharing of an individual files, but University of Leeds IT recommend the use of Teams / SharePoint where a project requires ongoing collaboration on or sharing of files.

The following links provide the latest University of Leeds information about commonly used sharing platforms, and also guidance around data classification and what you can store, and where.

- See <https://dataprotection.leeds.ac.uk/managing-electronic-data/> for an overview of managing electronic data
- See <https://dataprotection.leeds.ac.uk/wp-content/uploads/sites/48/2019/05/Information-Management-Guide.pdf> for guidance around data classification and what you can store where
- See <https://dataprotection.leeds.ac.uk/wp-content/uploads/sites/48/2019/05/Commonly-used-sharing-platforms.pdf> for details of commonly used sharing platforms

Your personal M-Drive is also currently available to use a backed up drive, but it is not possible for others to access data on this. The N-Drive is a further shared drive, although access for external collaborators through the N-Drive is managed centrally. Please also note that the M-Drives and N-Drives are currently scheduled to be phased out at the University of Leeds during 2023.

At the University of Sussex, the recommended place for data storage is box.com. Staff and research students at Sussex can store an unlimited amount of files and data by logging on to [sussex.box.com](https://www.sussex.ac.uk/its/services/networkandstorage/box) with a University account. Box is safe to use and is GDPR compliant. Box includes a versioning feature, allowing you to navigate back to a previous version of a file. Deleted files are also recoverable for 30 days after deletion.

A guide to box.com for University of Sussex staff is here:

<https://www.sussex.ac.uk/its/services/networkandstorage/box>

Transcribing data

If you are gathering qualitative data, you should generally transcribe these as text files for the purposes of archiving and sharing.

Digit data will, generally, be archived at the end of a project in the UK Data Service. Below, we present key guidelines from the UKDS in transcribing qualitative data. Further detail is available here: <https://ukdataservice.ac.uk/manage-data/format/transcription.aspx>

Following these guidelines will help with the archiving of data at the end of a project:

Transcripts should have:

- a unique identifier, a name or number
- a uniform and consistent layout throughout a research project or data collection
- a document header or cover sheet with interview or event details such as date, place, interviewer name and interviewee details
- speaker tags to indicate the question/answer sequence or turn-taking in a conversation
- line breaks between turn-takes
- numbered pages
- pseudonyms to anonymise personal identifying information

You should also:

- provide a transcriber with clear guidance and instructions with required transcription style, layout and editing, especially if multiple transcribers carry out work.
- anonymise data during transcription, or mark sensitive information for later anonymisation
- for non-English interviews, provide a translation or at least a summary of each interview in English, besides the transcriptions in the original language
- use automatic speech recognition (ASR) software designed to automatically transcribe text from an audio source with caution and check the result: these require significant training and calibration to recognise a particular voice, accent and dialect, but can be useful if interviews are similar and avoid any peculiar jargon
- before sending audio recordings and transcripts that contain personal or sensitive information to a transcriber, draw up a non-disclosure/confidentiality agreement with the transcriber and encrypt files before transfer. A template of an agreement from the UKDS can be found here: <https://www.ukdataservice.ac.uk/media/622354/ukda-transcriber-confidentiality-agreement.pdf>

Sharing and reusing your data

Guidance from ESRC, UKDS and Universities of Leeds and Sussex indicates that before sharing or reusing data you should consider:

- Do you have appropriate consent to share data and /or necessary agreement with third party project partners?
- Have you obtained copyright clearance from the data owner to archive data if using secondary data?
- Is data appropriately anonymised?
- Should access to data be restricted or only made available under certain conditions e.g. if you have signed a non-disclosure agreement?
- Are you currently publishing papers based on the data? Be aware of your publisher and funder expectations. You may need to make data available – not necessarily openly – where it underpins a publication.
- Are you gathering confidential data that is suitable for sharing, and have you recorded this and informed your University and funder?
- Have you agreed with partners what data will be shared? This includes deciding what will be subject to controlled conditions, what those conditions will be, how data will be discovered and accessed.
- Have you stated any collaborative research partner(s) and that a data sharing agreement exists in any ethical review applications?
- Have you decided what data should be kept and for how long?

Have you identified and documented any potential risks and vulnerabilities to sharing your research data e.g. participant disclosure risk and documented your decisions in your Data Management Plan?

Archiving your data

We expect that all Digit and Digit-funded data will be archived, where this is permitted in individual projects, in the UK Data Service. The UKDS is a leading data repository and placing all Digit data in the UKDS no later than 6 months after the end of a specific research project undertaken as part of Digit, but no longer than 3 months after the end period of funding for the Digit centre (31 December 2024). The use of the UKDS will maximise visibility and usability of the data by future research communities. There is an expert archiving team at the UKDS, as well as a big community of users who support and access data from the archive. Datasets in the UKDS are easy to find, and there are flexible conditions for depositing data, to respect embargo periods, and a variety of license reuse options.

Links to data records and metadata of files from Digit available at the UKDS will be provided from the Digit Data Observatory Webpages. You may also wish to provide links and metadata records to your own institutional research repository. However, raw data files will not be stored by Digit – archiving of all data will be through the UKDS.

Before archiving data, you should consider whether you want, and need to keep all your data, or whether some should be destroyed. The best approach is to think carefully, abide by policies (e.g. from funders) and document any decisions made and the reasons for them.

This guidance from the University of Sussex⁶ is useful when considering what you should keep and what you should get rid of:

- What data does my funder or the university require me to keep?
- Is the data 'vital' to the project or organisation?
- Do I have the legal and intellectual property rights to keep and re-use this data?
- Is there sufficient documentation to explain the data, and allow the data or record to be found wherever it ends up being stored?
- If I need to pay to keep the data, can I afford it?

Preparing data for archiving: UK Data Service guidance

Below is the guidance from the UK Data Service for preparing data for archiving – more detail is available at: <https://www.ukdataservice.ac.uk/deposit-data.aspx>

There is also a YouTube video that helps with the process of ReShare here, and would recommend watching before depositing: <https://ukdataservice.ac.uk/help/deposit-data/self-deposit-data-to-reshare/>

Study level documentation

Study-level documentation provides high-level information on the research context and design, the data collection methods used, any data preparations and manipulations and

⁶ <http://www.sussex.ac.uk/library/researchdatamanagement/store/selectingwhattokeep>

summaries of findings based on the data. This documentation is key to enabling the secondary user to make informed use of the data.

Good study-level data documentation includes information on:

- research design and context of data collection: project history, aims, objectives, hypotheses, investigators and funders
- data collection methods: data collection protocols, sampling design, sample structure and representation, work flows, instruments used, hardware and software used, data scale and resolution, temporal coverage and geographic coverage, and digitisation or transcription methods used
- structure of data files, with number of cases, records, files and variables, as well as any relationships among such items
- secondary data sources used and provenance, for example, for transcribed or derived data
- data validation, checking, proofing, cleaning and other quality assurance procedures carried out, such as checking for equipment and transcription errors, calibration procedures, data capture resolution and repetitions, or editing, proofing or quality control of materials
- modifications made to data over time since their original creation and identification of different versions of datasets
- for time series or longitudinal surveys, changes made to methodology, variable content, question text, variable labelling, measurements or sampling, and how panels were managed over time and between waves
- information on data confidentiality, access and any applicable conditions of use
- publications, presentations and other research outputs that explain or draw on the data

Data documentation can exist in reports to funders, technical reports, working papers, lab books or publications. Important data documentation is original questionnaires, interviewer instructions, interview topic guides or experimental protocols.

For each data collection deposited a 'read me' file will be needed:

https://www.ukdataservice.ac.uk/media/622352/readme_template.docx

You should also consider sharing and archiving and original software and code that you have generated and written as you have gathered and analysed data. There is increasing recognition of the value of managing and sharing code as well as data. Further guidance on this can be found from the UKDS here: <https://www.ukdataservice.ac.uk/manage-data/document/data-level>

When thinking about long term access and preservation of data, the following table produced by UKDS is helpful:

<https://www.ukdataservice.ac.uk/manage-data/format/file-formats.aspx>

You should contact the Digit Centre Manager and the Data Observatory lead prior to any depositing of data. This is because Digit needs to know when data is being deposited, and links to the deposited data, for inclusion in the Data Observatory. Also, they can offer some support if there are specific questions you have after having read this document.

Preparing your data for deposit: ReShare guidance

Please note that we would like to group data emerging from the Digital Futures at Work Research Centre. As you go through the process of 'ReShare' you will get to a point where they ask you about Data Collection. They ask for a Data Collection Title and also an Alternative title. For all Digit-funded research, please put 'Digital Futures at Work Research Centre' as the Alternative title. If this poses any problems, please contact Digit to discuss.

These are the guidelines as indicated by the UK Data Service when depositing your data through ReShare:

- group your data files in zip bundles according to their content or file format, to make upload and download easier, e.g. a zip bundle of interview transcripts, a zip bundle survey data files
- for large collections, keep a folder structure for the files in your zip bundle
- check recommended file formats before uploading files:
<https://www.ukdataservice.ac.uk/manage-data/format/recommended-formats>
- give files **meaningful names** that reflect the file content, avoiding spaces and special characters
- check that data files contain no disclosive information; to anonymise:
 - remove names or use pseudonyms
 - remove addresses and detailed location
 - change date of birth to year or create aggregate age groups
 - remove names and disclosive information from 'file properties', e.g. using MS Word Document Inspector
 - beware of hidden tracked changes in text or table files
- create a ReadMe file (txt format) for your data collection, with:
 - for each filename a short description of what data it includes
 - any relationships between the data files
 - for tabular data definitions of column headings and row labels, data codes (including missing data) and measurement units
 - for textual data a data list of all interviews, focus groups, etc. (see below)
- prepare essential documentation to upload with your data:
 - your ReadMe file (see above)
 - clear variable descriptions and code labels in each data file

- questionnaire form or data dictionary for surveys
- topic list for interviews
- consent form and information sheet used
- methods description
- [data list](#) of interviews
- PDF of website materials

Licensing your data: UK Data Service Licence Framework and Three-tier Access Policy

While data should be made available open where possible, safeguards might need to be put in place to protect participants.

At the UK Data Service, data are classified according to the consent used, their level of detail, sensitivity and confidentiality. The below options are offered:

[Open data \(Creative Commons licences\)](#)

These data are made available to any user without the requirement for registration for download. Suitable for data that contain no personal or disclosive information or data with agreement to publish personal details.

[Safeguarded data](#)

These data are made available for download to registered, authenticated users. Where appropriate, safeguarded data are made available only with the permission from the data owner or their nominee. Suitable for anonymised data with a potential minimal risk of disclosure.

[Controlled data](#)

These data are made available to registered, authenticated and accredited users, with projects approved by the data owner(s) via a secure virtual private network (data cannot be downloaded). Suitable for data considered personal data or personal information, or for data that are particularly sensitive, commercially or otherwise.

You may wish to consider making different versions of the same data available under different access arrangements.

[Further guidance on preparing data for archiving](#)

Specific guidance on preparing documentation for quantitative data can be found here:

<https://www.ukdataservice.ac.uk/manage-data/document/data-level/tabular.aspx>

Guidance for documentation needed with qualitative data here:

<https://www.ukdataservice.ac.uk/manage-data/document/data-level/qualitative.aspx>

Guidance for secondary data can be found here: <https://www.ukdataservice.ac.uk/manage-data/document/data-level/secondary.aspx>

The UK Data Service End User License can be found here:

<https://www.ukdataservice.ac.uk/media/455131/cd137-enduserlicence.pdf>

Appendix A: Checklist of University policies on research data at the University of Leeds⁷

- [University Information Protection Policy \(IPP\)](#): this sets out the requirements around the safe sharing of unclassified, confidential, and highly confidential data.
- [University risk assessment for security of data](#)
- [Data protection at the University](#)
- [Research ethics policy and ethical approval](#)
- [Professional integrity in research](#)
- [Informed consent protocol](#)
- [Policy on safeguarding children, young persons and adults in vulnerable circumstances \(PDF\)](#)
- [Research data management policy](#)
- [ICO anonymisation code of practice](#) [UK Anonymisation Network \(UKAN\) website](#).

⁷ <https://ris.leeds.ac.uk/research-ethics-and-integrity/other-resources/collecting-research-data/>
https://library.leeds.ac.uk/info/14062/research_data_management/63/safeguarding_data/2

Appendix B: Checklist of University Policies on Research Data at the University of Sussex⁸

- [Research Governance and Ethical Review Framework](#)
- [Procedure for the Investigation of Allegations of Misconduct in Research](#) (June 2019)
- [Use of The University's Name](#)
- [Policy on Internal Review of Research \[PDF 30.91KB\]](#) (July 2009) (only accessible to Sussex researchers)
 - and [Associated Operational Guidance produced by the University Working Group \[PDF 870KB\]](#) (April 2011)

Research Data, Publications and other Outputs

See also the [guidance and support offered by the University of Sussex Library](#).

- [University of Sussex Statement on Open Access to Research \(March 2015\) \[PDF 57.46KB\]](#) (March 2015), and the updated [Open Access for UKRI-funded researchers](#). (For further guidance on Open Access, see the Library's [OA support webpages](#)).
- [Sussex Research Online Policies](#) (managed by the Library - October 2017)
- [REF Open Access Exceptions Process](#) (Sept 2018). See also the Sussex [Library webpage on open access and the REF](#).
- [Research Data Management Policy](#) (October 2014, will be updated soon). (See also the Research Data Management [guidance from the Library](#)).
- The [San Francisco Declaration on Research Assessment \(DORA\)](#), to which the University of Sussex is a signatory.
- [Guidance on the use of External Research Advisors \(ERAs\)](#) in research assessment (March 2016).
- [Code of Practice for Research Assessment](#) (February 2017).
- [University Privacy Notice](#), which sets out the University's approach to data processing (May 2018).
- [Information classification and handling matrix](#) (Feb 2021)

⁸ http://www.sussex.ac.uk/staff/research/rqi/rqi_information_and_support/rqi_strategy_policy/research-policies

- Further policies, if you are not finding what you need above, can be found here:
<https://www.sussex.ac.uk/infosec/policies>

Appendix C: Links to useful resources at UKDS, UKDA and ESRC

ESRC Useful resources (Professional ethics codes and guidelines, templates and forms, and further information): <https://esrc.ukri.org/funding/guidance-for-applicants/research-ethics/useful-resources/>

UK Data Archive resources: <https://www.data-archive.ac.uk/resources/>

UK Data Service

- [Advice for new users: https://www.ukdataservice.ac.uk/help/new-user.aspx](https://www.ukdataservice.ac.uk/help/new-user.aspx)
- [Prepare and manage data: https://ukdataservice.ac.uk/manage-data](https://ukdataservice.ac.uk/manage-data)
- [Tools and templates for researchers can be found here https://www.ukdataservice.ac.uk/manage-data/tools-and-templates.aspx](https://www.ukdataservice.ac.uk/manage-data/tools-and-templates.aspx)
- [Guidance for collaborative research can be found here https://www.ukdataservice.ac.uk/manage-data/collaboration.aspx](https://www.ukdataservice.ac.uk/manage-data/collaboration.aspx)
- [UK Data Service regularly run training events covering all these issues which are advertised here: https://www.ukdataservice.ac.uk/news-and-events/events.aspx](https://www.ukdataservice.ac.uk/news-and-events/events.aspx)