A Practical Guide to Research Data Management & Data Management Plans (DMPs)

Document Reference and Version No:	Version 3 (New Format)
Purpose:	To assist researchers in better understanding the area of Research Data Management and in meeting funders' requirements in devising a Data Management Plan (DMP).
Date of Next Review:	1st May 2025
Who Needs to Know About this Document:	All SETU researchers
Revision History:	▪ Created May 2017: Eimear Fitzpatrick ▪ Revision 1 – May 2020: Philomena Treacy, Michelle Foley, Corina Power & David Kane ▪ Revision 2 – May 2024: Geraldine Canny, Michael Kugel, Luke Power, Éadaoin Butler, Alex Soikans
Document Author:	Office of Research, Innovation & Impact
Document Owner:	Office of Research, Innovation & Impact

HR EXCELLENCE IN RESEARCH

Table of Contents

Introduction

In this information age, it is possible to manage research data digitally and to make it reusable for other researchers to build upon. Openness should be the default position for most research data. By being subject to scrutiny by other researchers, open data promotes research integrity. Research data should also be as closed as necessary – subject to legal and privacy considerations. All of this requires planning.

The purpose of this guide is to assist researchers in better understanding the area of Research Data Management and in meeting funders' requirements in devising a Data Management Plan (DMP). An increasing number of national and EU funding agencies and schemes such as EU Horizon Europe require researchers to develop a detailed plan for managing, storing or preserving data, sharing their data with the general public and the secure destruction of data following relevant retention periods. Devising a Data Management Plan is also good research practice for you and your wider research team even when the data cannot be shared for various reasons - legal, privacy, secondary use, etc.

What is Research Data?

Research data can generally be defined as any representation or other objects that are created or gathered for the purposes of producing research or scholarship, and which can be used to validate or reproduce original research findings. The underlying research materials which support research publications can be described as research data. Research data can cover a diversity of form and content, including (but not limited to) numbers, text, images, audio, simulations, models, interview recordings, questionnaires, laboratory notebooks, videos, algorithms, codebooks, test results, specimens, databases or any combination of these. Data objects can be physical or print as well as digital, for example:

- Archaeological artefacts (of any size). These objects can be stored in museums themselves and be used to create different kinds of data (radiocarbon date, 3D scan, photograph, X-ray, etc.)
- Geological samples (similar to archaeological artefacts)
- Genetic – Cell lines like the HELA cells that were used for the study of cancer for many years
- Genetic – Specialist strains of animals (like the Drosophila strains kept at the Bloomington Drosophila Stock Center (https://bdsc.indiana.edu/index.html)
- Genetic – Plasmids are loops of DNA, useful for research, living bacteria. AddGene is an example of a centre that looks after these cell lines (https://www.addgene.org)

What is a Data Management Plan?

A DMP is a formal document that outlines how your data will be looked after both during the lifetime of your research project and beyond. Check the specific timeline requirements with your funding agency. The Principal Investigator (PI) has the overall responsibility to ensure the DMP is created and submitted to the funding agency as required.

The content of a DMP will vary but you will typically be asked to provide information about:

- the volume and type(s) of data you will generate
- how you will ensure that your data is well organised and adequately documented

- how you will make sure that your data is ethically and legally compliant including in line with General Data Protection Regulation (GDPR) principles
- where your data will be stored and backed up during the lifetime of the project
- how you will preserve your data and make it available for others to reuse (where appropriate) in the long term
- who will be responsible for looking after your data during and after the project and what resources will be needed.

Why do I need a Data Management Plan?

Most of the major funders require applicants to include a DMP with their application for funding. The Open Access Research Data Pilot (ORD) was run over selected areas of Horizon 2020 between 2014 and 2016. In 2017 it was extended to cover all thematic areas. The Commission acknowledges that there may be good reasons why data cannot be made available so there are opt-out possibilities at any stage: the grant application stage, during the grant agreement preparation stage and after the signature of the grant applications. Costs associated with open access to research data can be claimed as eligible costs from some funding agencies, check with your funding programme guidelines. In Ireland, the National Open Research Forum (NORF) was established in 2017. NORF led the publication of the National Framework on the Transition to an Open Research Environment (2019) and the development of the National Action Plan for Open Research 2022-2030.

Maintaining a DMP for your research project is good research practice. It can help you manage and look after your data throughout the lifetime of your research project and should be thought of as a "living" document that can be continually revised and updated to reflect your changing data management needs, e.g. add an '**update**' section under each action already described, reflecting on the original or latest version, rather than starting afresh each time.

What are the benefits of a Data Management Plan?

Having a DMP can save you time and resources by:

- making it easier to find and understand your data when you need to use or re-use it
- helping to manage risk (e.g. of data loss; of accidental or malicious disclosure of sensitive or confident data)
- identifying tasks and responsibilities that need to be planned for in advance (e.g. managing ethical and legal obligations)
- identifying in advance any extra costs and resources needed for carrying out data management activities such as data security

What to consider before devising a Data Management Plan

The DMP will deal with the following questions among others.

1. What research data am I creating or collecting?
2. Who will be responsible/take ownership of each aspect of the plan?
3. What policies (funder/institutional) will apply to the plan?
4. How will the data be organised (file naming conventions, file versioning)?
5. How will data be anonymised if necessary?

6. How will the data be documented during the collection and analysis stages of the research?
7. How will I backup, store, secure and manage access to my data?
8. What equipment and facilities are needed?
9. How will I manage any ethical issues?
10. Who will have ownership/rights to my data (especially important if this is collaborative research) (or collected as part of industry-funded research)?
11. Who will have access to the data I have collected?
12. How will I preserve the data once the research project is finished?
13. How will the data be destroyed following the necessary retention periods?

Your plan will cover initiation of the research, mid-term review and final review. Remember your plan, like your research, will evolve and may need amending as the direction of the research changes.

Ethical Considerations

Ethical and legal requirements may apply to the management of research data, particularly if the research involves people. Ethical considerations include the purpose and nature of the research itself. Research data about people can be shared ethically and legally if researchers avail of informed consent, anonymisation and controlled access.

GDPR Considerations

Personal data relates to information which relates to a living individual who is identifiable either directly from the data itself or from the data in conjunction with other information held by SETU. If personal data is gathered, how will compliance with GDPR requirements be ensured?

Ensure that when dealing with personal data the main principles are adhered to including:

- Processing personal data fairly, lawfully, and in a transparent manner (Principle of Lawfulness, Fairness, and Transparency);
- Obtaining personal data for specified, explicit, lawful, and legitimate purposes, and not processing it further (Principle of Purpose Limitation);
- Ensuring personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they were gathered (Principle of Data Minimisation);
- Ensuring personal data is accurate, and where necessary kept up to date (Principle of Accuracy);
- Ensuring personal data is not stored for longer than is necessary (Principle of Data Storage Limitation);
- Ensuring personal data is processed in a secure manner, which includes having appropriate technical measures in place to: prevent and / or identify unauthorised or unlawful access to, or processing of, personal data; and prevent accidental loss or destruction of, or damage to, personal data (Principles of Integrity and Confidentiality;
- Ensuring that data controllers take responsibility for, and can demonstrate compliance with, the other principles of data protection (Principle of Accountability).

Transfers of personal data to third countries (outside the European Economic Area) require certain safeguards.

In addition, you should also consider the following:

- gaining informed consent for preservation and/or sharing of personal data.
- anonymisation of personal data for preservation and/or sharing (irreversibly anonymous data is no longer considered personal data and is outside the remit of GDPR).
- pseudonymisation of personal data (the main difference with anonymisation is that pseudonymisation is reversible).
- encryption which is seen as a special case of pseudonymisation (the encryption key must be stored separately from the data, for instance by a trusted third party).
- whether there is a managed access procedure in place for authorized users of personal data.
- the rights of data subjects under GDPR regulations including access, rectification, erasure and restricting processing.

Special category personal data (sensitive personal data) are subject to additional protections under GDPR and may only be processed in limited circumstances set out in Article 9. Special category data are data concerning: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data processed for the purpose of uniquely identifying a natural person, health, a natural person's sex life or sexual orientation.

FAIR Data

It is not enough to put raw research data onto a server in an un-annotated format that nobody can use outside your project. Properly open data, as stipulated by funder mandates, is FAIR data. FAIR stands for Findable, Accessible, Interoperable and Reusable. Following the lead of the European Commission and Horizon Europe, Irish funders, including the Health Research Board (HRB) and Irish Research Council (IRC) are now asking Irish researchers to address, via a DMP, how they will make their data FAIR.

The FAIR Data Principles were developed and endorsed by researchers, publishers, funding agencies and industry partners in 2016 and are designed to enhance the value of all digital resources.

- **Findable** – It should be possible for others to discover your data. Rich metadata should be available online in a searchable resource, and the data should be assigned a persistent identifier.
- **Accessible** – It should be possible for humans and machines to gain access to your data, under specific conditions or restrictions where appropriate. FAIR does not mean that data need to be open! There should be metadata, even if the data aren't accessible.
- **Interoperable** – Data and metadata should conform to recognised formats and standards to allow them to be combined and exchanged.
- **Reusable** – Adequate documentation is needed to support data interpretation and reuse. The data should be clearly licensed so others know what kinds of reuse are permitted.

If your goal is to make your data FAIR you should build this into your research plan from the start. What resources (for example financial and time) will be dedicated to data management and ensuring that data will be FAIR (Findable, Accessible, Interoperable, Re-usable)?

- Explain how the necessary resources (for example time) to prepare the data for sharing/preservation (data curation) have been costed in. Carefully consider and justify any resources needed to deliver the data. These may include storage costs (hardware/ software), staff time for preparing data for deposit to make it FAIR and repository charges.
- Indicate whether additional resources will be needed to prepare data for long term storage or "archival" or to meet any charges from data repositories. These costs are usually borne by the Institution but perhaps in the case of very large datasets, particular arrangements would have to be made with a repository provider. If yes, explain how much is needed and how such costs will be covered.

Checklists

It is recommended that you use the SETU Data Management Checklist (See Appendix A) to ensure that you cover all the essential areas.

Data Types/ Models

- Text (e.g. doc, txt, pdf)
- Numerical (e.g. SPSS, STATA, .xls, Access, MySQL)
- Multimedia (e.g. jpeg, tiff, wav, mpeg, quicktime)
- Models (e.g. 3D, statistical)
- Software (e.g. Java, C)
- Domain-specific (e.g. FITS in astronomy, CIF in chemistry)

Compiling a Data Management Plan

Instru

You can use an online tool like the DMPonline from the Digital Curation Centre in the UK. This is highly recommended as it gives examples of DMPs in a number of disciplines as well as allowing you to share your plan with others in your research group and they can contribute to the plan too. This software will also allow you to manage your plan.

You do not need to be UK-based to use DMPonline, but you must register. The registration form has a pre-determined list of organisations. Choose "Other" and fill in South East Technological University. The software will prompt you through the process.

What to cover in your Data Management Plan

Data summary

- State the purpose of the data collection/generation.
- Specify the method of data collection.
- Explain how the data relates to the objectives of the project.
- Specify the types and formats of data generated/collected.
- Specify if existing data is being re-used (if any).
- Specify the origin of the data.
- State the expected size of the data (if known).
- Describe how this data might be useful to others.

Making your data FAIR

Making data findable, including provisions for metadata

- Outline the discoverability of data (metadata provision).
- Outline the identifiability of data and refer to standard identification mechanism. Do you make use of persistent and unique identifiers such as Digital Object Identifiers?
- Outline naming conventions used.
- Outline the approach towards searching for keywords.
- Outline the approach for clear versioning.
- Specify standards for metadata creation (if any). If there are no standards in your discipline describe what type of metadata will be created and how.

Making data openly accessible

- Specify which data will be made openly available. If some data is kept closed provide the rationale for doing so.
- Specify what methods or software tools are needed to access the data. Is documentation about the software needed to access the data included? Is it possible to include the relevant software (e.g. in open-source code)?
- Specify how and where the data and associated metadata, documentation and code are deposited.
- Specify how access will be provided in case there are any restrictions. For certain sensitive datasets, particularly in health, access to anonymised datasets may be given on a case-by-case basis.

Making data interoperable

- Assess the interoperability of your data. Specify what data and metadata vocabularies, standards or methodologies you will follow to facilitate interoperability.
- Specify whether you will be using standard vocabulary for all data types present in your data set, to allow inter-disciplinary interoperability? If not, will you provide mapping to more commonly used ontologies? An ontology, in this case, is the commonly agreed and understood language for the naming of things, their properties and relationships. You may choose to stay with your discipline-specific ontology, or you may choose to use more commonly used set of terms to describe your data. Whatever you choose, you must be guided by the need to make the data as understandable to as many as possible, without losing any meaning.

Making data re-usable

- Increase data re-use (through clarifying licenses). Example of a data license: Creative Commons License. Specify how the data will be licenced to permit the widest reuse possible.
- Specify when the data will be made available for re-use. If applicable, specify why and for what period a data embargo is needed.
- Specify whether the data produced and/or used in the project is useable by third parties, after the end of the project? If the re-use of some data is restricted, explain why.
- Describe data quality assurance processes.
- Specify the length of time for which the data will remain re-usable.

Allocation of resources

- Estimate the costs for making your data FAIR. Describe how you intend to cover these costs.
- Clearly identify responsibilities for data management in your project.
- Describe costs and potential value of long-term preservation.

Data security

- Address data recovery as well as secure storage and transfer of sensitive data including any necessary data-sharing agreements to be completed.

Ethical aspects

- To be covered in the context of the ethics review, ethics section of Description of the Action (European funding), and ethics deliverables. Include references and related technical aspects if not covered by the former.

Other

- Refer to other national/funder/sectoral/departmental procedures for data management that you are using (if any).
- How you are going to address the data protection implications under the GDPR & Data Protection Act legislation.

Data Management Plan for a Research Grant Application

Increasingly funders are mandating that data must be made openly available as well as publications resulting from the data. For example, in Horizon Europe, awardees must manage their data in line with FAIR principles. See here for further information.

What do funders expect from the preliminary outline?

Funders typically expect a succinct summary submitted as part of the "case for support" or in an allocated section of the application form. A funder will expect a DMP to outline how the data will be created, managed, shared and preserved - justifying any restrictions that have been applied.

- **Consult and collaborate widely:**
  Ask for advice from colleagues, the Research Support Unit (RSU), the Library, Computer Services and the Ethics Committee (See Appendix B for Assistance within SETU).
- **Justify your decisions:**
  Generally the funder will not specify particular file formats, standards or methodologies that you are expected to use. However, you need to choose and demonstrate that the selections you have made are the appropriate ones, both for the project and for the future. You also will need to make a convincing case with regards to restrictions on data sharing.
- **Be prepared to implement:**
  You need to convince the funder that you understand their requirements and have realistic plans in place to meet these. These plans should be clear and achievable. Clearly defined roles and responsibilities will help so be very clear about who will do what, how and when.

Content:

- Detail what data you will create and explain why you have opted for particular formats, standards and methodologies. Be aware that the choices you make here will make it easier or harder to share your data. Using standard or widely adopted formats will make your data interoperable and more easily shared. Open or non-proprietary data formats are preferable. If you are depositing your data into a subject/discipline or institutional archive, check what the preferred formats are.
- You will need to state the data outputs you expect to generate. This means stating the volume, type, content, quality and format of the final dataset. Outline the metadata, documentation or other supporting material that must accompany the data for it to be understood properly. State the standards and methodologies that you will use to collect and manage this data.
- Point out the relationship to other data available in other repositories; existing data sources that will be used, gaps between available data and your research project, the added value that your data will provide in relation to existing data.

Documentation and metadata

- This is important as it allows your data to be understood and discovered by others. You must capture the contextual details about how and why the data was created. Metadata describes the data in detail (think of it like a description in a catalogue). There are various standards that can be used for this, check with David

Kane (Waterford campus) or Breda Connell (Carlow campus) in the library or your colleagues for the one most appropriate for your discipline.

Make a strong case for any restrictions on sharing

- You should justify any embargo periods or restrictions on sharing your data. Remember there is an expectation that publicly funded research data will be openly available as soon as possible.
- If using human subjects, you will be guided by formal ethical review and outline the steps you will take to protect the research participants. Show that you have weighed up the reasons to share or not share and, in this context, negotiated informed consent of the participants may be one way forward. You should also show that you are aware of relevant legislation such as the Data Protection Acts; talk to the Data Protection Office at SETU.

Data ownership

Show that you are aware of this issue. You must demonstrate that you have looked for advice on and addressed all copyright, license or other rights issues that might arise; consult with the SETU Technology Transfer Office (TTO).

Anticipate how other users might avail of your data

If you can, anticipate the type of users who might avail of your data and address their needs when deciding how to make the data available. Remember your objective is to make it as easy as possible for them to access the data. The funders will welcome clarity around access so be clear about where, when and how your data will be made available. You may want to license your data using, for example a Creative Commons License . Where possible use an appropriate disciplinary database, data centre and the SETU institutional repository or a cross disciplinary database like Fig share. For research funded by the European commission Open Research Europe should be used. GitHub is a free platform for sharing software code.

Security:

Describe how you plan to securely store the data. Security will need to be stronger for any sensitive data you collect. If you are using an online server know where your data is housed and if this is legally permissible. The more important your data and the more it is used, the more regularly it needs to be backed up. If your project has multiple partners, specify the responsibilities for data management and curation within the research teams operating in all partner institutions; outline in the Consortium Agreement.

Appendices

Appendix A: SETU Data Management Checklist

Please use this checklist as a guide to help you develop a research Data Management Plan (DMP) for your research project.

Not all sections/questions will be relevant to your project, simply use this document as a starting point to help you structure your planning process.

PROJECT DESCRIPTION:

- Project title
- The aim/purpose of the research
- Project duration

CONTEXT:

Administrative and contact information

- Principal investigator (PI)
- Researchers/other project members
- Main contact details
- Collaborators/partner institutions
- Funding source(s) and requirements

DATA TYPES:

Provides a description of the data your project will capture, create or use. It is important to record this detail to help you and subsequent users understand why and how the data was created.

- How will data be created (captured)? E.g. interview data, questionnaires, imaging, experimental measurements etc.
- What data formats will be used? E.g. file formats such as Excel, Word, open source etc.
- Consider choice of data formats such as: will the data formats meet certain specifications including international or national standards, widely used, is it accepted as best practice in this discipline, will it facilitate re-use?
- Will the data be reproducible? What would happen if it got lost or became unusable later?
- How much data will there be and what will its growth rate be? How often will it change?
- Will existing data be used? If so, from where, and what is the relationship to the existing data?
- Are there special tools or software needed to create/process/visualise the data?
- Are these tools or software General Data Protection Regulations (GDPR) compliant?
- How will metadata be captured, created and managed?
- How will your data be compliant with the GDPR?

DATA ORGANISATION, DOCUMENTATION AND METADATA:

Organising, documenting and describing data is important in order to assure quality control and reproducibility of data

- What metadata standards will be used?
- How will metadata be captured, created and managed? Is there a discipline-specific standard?
- How will folders and files be structured and named?
- How will different file versions be managed?
- What data identifiers will be assigned?
- What other documentation and contextual information will be available in order to help others understand the data? E.g. data dictionaries, codebooks, questionnaires.

DATA STORAGE AND SECURITY:

- **Storage**
  - Where and what media? Short-term, longer-term?
  - Who will be responsible?
- **Back-up**
  - How will it be done and how often will it be done?
  - Who will be responsible?
- **Security**
  - How will data security be guaranteed e.g. data encryption, password etc.
- **Sharing**
  - How will the data be shared during the project? This is different to how the data will be shared long-term (archival of FAIR data on a repository)
- **Access**
  - Who will have access to the data during the lifetime of the project?

File Naming Best Guidance:

You should use consistent, unique and descriptive file and folder names when saving research data. This will help you to keep track of your data files and share data among the team.

Sample Naming Conventions might include:

- Version number
- Project acronym
- File status
- Date
- Topic
- A set order of information e.g. YYYYMMDD for dates

LONG-TERM PRESERVATION:

- What data will be kept or destroyed after the end of the project?

- How long will data be kept? e.g. 3-5 years, 10-20 years, permanently (giving consideration to retention periods of the University & GDPR requirements)?
- Where will the data be stored? e.g. archive, data repository, network etc.
- What file formats will be used? Are they long-lived?
- Who will manage the long-term data?
- What is needed to prepare the data for preservation or data sharing?
- What related information will be deposited with the data?
- Who will be responsible for the destruction of the data following the necessary retention periods?

ETHICS, GDPR AND INTELLECTUAL PROPERTY:

- Are there any ethical and privacy issues that may prohibit sharing of some or all of the data? If so, how will these be resolved and/or managed?
- Does your data contain confidential or sensitive information? If so, have you obtained informed consent for data sharing from the respondents from whom you collected the data?
- Who owns the data arising from your research, and the intellectual property rights relating to them? This is particularly important if your project is cross-institutional as ownership needs to be clearly established from the beginning. Also, if you are using facilities offered by journal publishers to store your data they may have assumed ownership rights.
- Are there ethical or legal reasons why you cannot share the data? For example, did you tell the interviewees that the data would be anonymised and shared and in this regard, remember there are extra responsibilities under the GDPR.

DATA SHARING AND RE-USE:

- In addition to the owners of the data you generate, who else has a right to see or use this data? And who else should reasonably have access? Who will be the audience for your data?
- Are there any limits to data sharing required?
- Are there any sharing requirements? E.g. funder data sharing policy or a data transfer agreement
- How will the data be discovered and shared?
- What tools / software will be needed to work with the data?
- Will there be embargo periods?

IMPLEMENTING YOUR PLAN:

- Who will be responsible for ensuring your plan is followed?
- How often will your plan be reviewed and updated?

Transfer of personal data outside the EEA

Transfers of personal data to third countries require certain safeguards. Personal data must not be transferred to a third country unless there are adequate safeguards in place which will protect the rights and freedoms of the data

subject. It is important to note that this also covers personal data stored in the cloud as infrastructure may be in part located outside of the EEA.

Functions must not transfer personal data to a third party outside of the EEA regardless of whether the University is acting as a Data Controller or Data Processor unless certain precautions are taken. It is the responsibility of the person or persons involved in the data processing and transfer of personal data to ensure that the third party outside of the EEA conforms to the rigorous data protection principles and conditions of GDPR and is covered under the 'adequacy decisions' made by the European Commission. An 'adequacy decision' refers to a decision by the commission as to the safety of transferring data to certain countries outside of the EEA.

Since 2019 the Commission has made an 'adequacy decision' to approve the transfer of personal data to the following countries and territories: Andorra, Argentina, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, United Kingdom, and Uruguay.

Additionally, the Commission made decisions about other countries with some restrictions as follows:

1. The transfer of personal data to Canada only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA.
2. The transfer of personal data to the USA is only for personal data transfers covered by the EU-US Privacy Shield framework. The Privacy Shield places obligations on American organisations certified by the scheme to protect personal data and allows for a redress system for data subjects.

If you wish to transfer personal data to an American company under the Privacy Shield, you should:

1. Consult the Privacy Shield list to see if the company is currently certified; and
2. Ensure the certification covers the type of data you want to transfer.

Appendix B: Assistance within SETU

Data storage, backup and security:

SETU's IT support team is happy to discuss the options available to you regarding data storage or any of your IT requirements, contact: computerservices@setu.ie

FAIR data:

You should also contact Alex Soikans at the Research Support Unit for queries relating to FAIR data, open access research and DMPs. Colleagues at the library can be contacted about the institutional publications repository.

Intellectual property:

For queries regarding intellectual property and support for researchers interested in commercialisation please contact James O' Sullivan at the Technology Transfer Office.

Research ethics committee:

Contact ethics@setu.ie

Research integrity:

Contact Dr Kim Murphy (from September 2024)

Data protection:

Contact SETU's Data Protection Officer, Paula Butler

Data management plans for research grant applications:

For queries regarding data management plans for research grant applications contact the Research Support Unit. Researchdata@setu.ie

Appendix C: Useful Resources

- Digital Curation Centre: Data Management Checklist
- Digital Curation Centre: Funders' data plan requirements
- Digital Curation Centre: Online Data Management Plan tool
- Digital Repository of Ireland: Resources for AHSS Researchers on Data Management
- European Research Council: Data Management Plan Template
- Guedj & Ramjoué (2015): European Commission Policy on Open-Access to Scientific Publications and Research Data in Horizon 2020
- Health Research Board: GDPR Guidance for Health Researchers
- Horizon 2020 Programme (2016): Guidelines on FAIR Data Management in Horizon 2020
- Horizon 2020 Programme (2016): Guidelines on Open Access to Scientific Publications and Research Data in Horizon 2020
- National Open Research Forum (2022): National Action Plan for Open Research
- Open AIRE: Open Science Guides
- Open DOAR: Directory of Open Access Repositories
- Open Research Europe: FAIR Data – A Quick Guide for Researchers
- Re3data: Registry of Research Data Repositories
- Research Data Alliance: Metadata Standards Directory
- ROAR: Registry of Open Access Repositories
- Science Europe (2018): Practical Guide to International Alignment of Research Data Management
- SETU: Research Policies & Procedures
- SETU Research Support Unit: Research Cross Cutting Themes & Resources
- UCD Library: Research Data Management Guidance
- University of Edinburgh: Research Data Management Training (free online tutorial)
- UK Data Archive (2011): Managing and Sharing Data – Best Practice for Researchers
- Wellcome Trust: How to complete an outputs management plan

Appendix D: Template Data Management Plan

Proposal Name

1. Description of the data

   Type of study

   1.1. Types of Data

   1.2. Format and scale of the data

2. Data collection and generation

   2.1. Methodologies for data collection and generation

2.2. Data quality and standards

3. Data management, documentation and curation

3.1. Managing, storing and curating data

3.2. Metadata standards and data documentation

3.3. Data preservation

Data will be deposited in the Data Portal of the SETU institutional repository https://repository.wit.ie/

4. Data security and confidentiality

5. Data sharing and access

6. Responsibilities and implementation

Author of the data management plan_____
Contact email_____

Date_____

- If you want to know more about Data Management there is a free online tutorial available from the University of Edinburgh https://mantra.edina.ac.uk. Guidance is also available in the SETU Research Cross Cutting Themes & Resources.

Disclaimer: This guidance has been prepared by the SETU Research Support Office to assist researchers in the development of a Data Management plan. It is intended to be general guidance and it is not legal advice.