Title:	Research Data Management Standard Operating Procedure		
Version:	1.2	**Effective Date:**	March 2021
Summary:	This Procedure defines requirements for managing research data		

1. Introduction and purpose

This standard operating procedure (**Procedure**) supports and should be read in conjunction with the University's Research Data Management Policy.

2. Scope and definitions

As per the University's Research Data Management Policy.

3. Roles and responsibilities

3.1 Researcher

Research study

1. For the purpose of this **Procedure**, all research is to be organised into distinct time-limited studies (**Study**) and for each **Study**, the University of Manchester participants must nominate, in advance, a principal investigator (**Principal Investigator**) for the University, who will take responsibility for ensuring good research data management practice.

2. For external collaborations where this University is not the lead institution, this University's Lead Co-Investigator is expected to assume the same responsibilities under this Policy as a **Principal Investigator**.

3. For research **Studies** undertaken by a postgraduate researcher, their main supervisor is expected to assume the same responsibilities under this Policy as a **Principal Investigator**.

4. For research **Studies** undertaken as part of a taught course, the course co-ordinator is expected to assume the same responsibilities under this Policy as a **Principal Investigator**.

5. The **Principal Investigator** has ultimate responsibility for ensuring the proper administration, oversight and security of research data relating to a research **Study**. In practice the responsibility for day-to-day management of research data may be passed on to other members of the **Study** team, and any shared responsibilities must be recorded in the Data Management Plan.

Data management planning

6. The **Principal Investigator** must ensure that a Data Management Plan is written before the research commences, adhered to and updated as necessary throughout the **Study** lifecycle.

7. All Data Management Plans must be recorded and maintained using the DMPonline service. For funded **Studies** a plan must be recorded using the funder's template where it is available. Where there is no funder template available, or where the **Study** is unfunded, the 'University of Manchester generic template' within DMPonline must be used.

8. All Data Management Plans in DMPonline are prefixed with the 'Manchester Data Management Outline' section. If a funder or sponsor does not require a fully completed Data Management Plan at the research application stage, then only the 'Manchester Data Management Outline' section needs to be completed at that stage.

9. When a Data Management Plan is created using DMPonline there is an option to download as PDF, and this must be attached to the relevant research approval form and, where relevant, the ethics application in the online ethical review application system (ERM). The downloaded PDF must include the 'Manchester Data Management Outline' section. If an Information Governance Risk Review is completed for a **Study** then the Data Management Plan must be shared with the relevant Information Governance Officer. The Getting started in DMPonline guide explains how to share a data management plan.

10. Researchers must take into account any likely costs for storing and managing their research data during the lifetime of the **Study**. The time and cost for storage and management must be explicitly written into research applications, including instances where data will need to be made publicly available or curated for many years beyond the **Study** lifetime.

11. It is not always appropriate to make research data openly accessible and there are valid reasons why access to research data must be restricted, including inter alia, to maintain confidentiality, guard against unreasonable costs, protect individuals' privacy, respect consent terms, as well as managing security or other risks. Researchers controlling or restricting access to data must justify their actions and explain how they have sought to limit restrictions in the Data Management Plan.

12. A Data Management Plan must be recorded or stored with other research **Study** documentation or with the research data for the purpose of the future management of the research data.

13. A Data Management Plan is a living document that must be reviewed whenever significant changes occur (e.g. to the storage locations of the data). In any event it is good practice to review DMP at least annually.

Ownership

14. A **Principal Investigator** is an **Information Store Owner** and must ensure that ownership of, and intellectual property rights in, all research data are agreed formally and documented before the research commences, paying due regard to the University's Intellectual Property Policy and relevant third party agreements, and reviewed and updated whenever appropriate. The documentation must also detail how ownership and storage of data and materials will be affected by researchers changing institutions, or withdrawing from a collaborative **Study**.

15. Funders and other stakeholders (e.g. research collaborators and research participants) may have intellectual property requirements and these must be considered by the **Principal Investigator** during data management planning.

16. Where a **Study** is conducted in collaboration with external research partners, researchers must work with the Contracts Team to ensure that suitable agreements for the ownership and use of research data are established and agreed in writing by the parties concerned before the **Study** starts.

17. Where a **Study** uses a data processor such as a cloud storage company, courier, or printing supplier, then researchers must work with the Contracts Team to ensure that data processing agreements are in place with the appropriate data protection clauses. Where a **Study** uses a data processor such as applications, communication tools or social media, then researchers must adhere to any relevant service terms and conditions.

Data Protection

18. To minimise the risk to information, and to protect the rights and privacy of any **Study** participants, researchers must align their processes with data protection legislation and principles.

19. To preserve the privacy of any **Study** participants, researchers must apply safeguards to personal information which are commensurate with its information security classification, as described by the Standard Operating Procedure - Information Security Classification, Ownership and Secure Information Handling.

20. Data protection training is mandatory for all University staff with an active IT account, and must be completed every two years. This training is available as an online course.

21. DMPonline is the University's Information Asset Register for research, so the **Principal Investigator** must ensure that the Data Management Plan accurately represents how the **Study** is using information.

22. Where a **Study** involves high risk processing activity such as using innovative technologies, or monitoring and tracking human research participants, researchers may be asked to complete a further assessment such as an Information Governance Risk Review or a full Data Protection Impact Assessment. More information on high risk processing is available from the Information Commissioner's Office website.

Storage

23. Whilst actively collecting and analysing research data, it must be stored in the University's secure Research Data Storage Service or in other storage that satisfies the University's Information Governance Risk Review. **Studies** can apply to the Research Data Storage Service for a limited amount of free storage, with additional storage available at a cost.

24. University employees, postgraduate researchers and students who do not have access to the Research Data Storage Service through a research **Study's Principal Investigator** may use their Personal Data Storage Service (P Drive) to store research data.

25. The pseudonymisation key for personal information must be kept separately and securely from data relating to research participants. The University provides guidance on encryption for keeping information secure.

26. **Studies** working with research data that is highly restricted or that require data storage in excess of 8 TB must contact Research IT for support and guidance.

27. The University strongly discourages the use of portable devices and media (such as laptops, external hard drives, local NAS servers and DVDs) which are vulnerable to failure, damage, loss and theft. There are exceptional circumstances, such as fieldwork, where portable devices and

media may be necessary to temporarily store or transfer data. Where such exceptions exist, data must be moved as soon as possible to University-approved systems. Where portable devices and media are used then:

a. temporary storage of Highly Restricted or Restricted information (such as personal information) outside of University-approved systems requires the file, device or media to be encrypted and the device or media to be kept physically secure at all times; and
b. researchers must take into account the need for regular backups. The Information Governance Office can advise whether such duplication of information is recommended for specific scenarios.

28. Researchers must identify non-digital data that is not suitable for digitisation and organise storage in a secure environment in accordance with the Records Management Policy.

Archiving, publishing and metadata

29. Research data that underpins a published research output must be deposited in a data repository or archive in a form suitable for long-term retention, and where possible wider publication where:
    a. a suitable repository is available;
    b. the data meets the criteria for deposit; and
    c. the data can be made available in ways that do not infringe legal or ethical restrictions.

30. Research data must be accompanied by metadata and documentation according to accepted norms and domain-specific protocols (where they exist) to allow others to discover, understand and re-use the data in the long term.

31. Research data must be accompanied by an appropriate licence so that others can understand what they are allowed to do with the data.

32. Where research data has been shared using a public repository the details of this must be recorded in Pure. If research data has:
    a. been assigned a Digital Object Identifier (DOI) then use the Research Data Gateway to submit the DOI. The Library will then add the metadata to Pure.
    b. not been assigned a DOI then use Pure to record details of the data.

33. Published research outputs must include information on how to access any supporting data. Citations to research data must comply with the Joint Declaration of Data Citation Principles.

34. Where research data is used to underpin published research, but there is good reason for the data not to be made openly available, it is nevertheless expected that researchers will normally make all relevant data and related materials available to other researchers or interested parties for the purpose of verifying the integrity of the research, subject, where necessary, to suitable restrictions and confidentiality undertakings.

Retention

35. Research data must be retained for as long as specified by research funder, legal and regulatory requirements, and for as long as they are of continuing value to the researcher and the wider research community. This includes research data that substantiates research findings or represents records of the University. Data that contains personal information must be anonymised as soon as possible regardless of the retention period.

36. In the absence of specific guidance on retention periods, research data that underpins findings in publications must be stored in accordance with the University's Records Management Policy and Records Retention Schedule.

37. When destruction of confidential data is required, it must be securely destroyed in accordance with the University's guidance on the disposal of confidential material.

Exit planning

38. If a researcher leaves the employment of the University the Staff Exit Checklist must be completed to ensure they pass on ownership of and access to any research data and any associated responsibilities as appropriate.

39. If a postgraduate researcher or student leaves the University then the Principal Investigator must ensure that the postgraduate researcher or student passes all research data owned by the University or external collaborators to the relevant owner including any password or other information required to access such data before they leave.

3.2 Head of Organisational Unit

1. It is expected that the **Head of Organisational Unit** (normally the Head of School or equivalent) will ensure in signing of a Research Application Form that relevant researchers are following good practice and complying with the University's Research Data Management Policy.

2. Should the **Principal Investigator** leave the University or be unable to continue in the role before all their duties relating to the data have been discharged, it is the responsibility of their **Head of Organisational Unit** to appoint a replacement.

4. Review of Procedure

This **Procedure** will be reviewed at least annually or when significant changes are required.

Version amendment history		
Version	Date	Reason for change
1.2	March 2021	Annual review and update

Contact List for queries related to this Procedure

Role	Name	Telephone	Email
Research Data Management Service team	Chris Gibson / Clare Liggins / Eleanor Warren	0161 275 7853	researchdata@manchester.ac.uk

Research Data Management Strategic Lead	Bill Ayres	0161 275 7853	bill.ayres@manchester.ac.uk
Associate Director, Research and Digital Horizons, University of Manchester Library	Lorraine Beard	0161 306 4918	lorraine.beard@manchester.ac.uk

Document Control

Procedure title:	Research Data Management Standard Operating Procedure
Date Approved	
Approving Body	Library Executive Team
Version	1.2
Supersedes	1.1
Previous Review Dates	March 2018, February 2019
Next Review Date	March 2022
Related Statutes, Ordinances & General Regulations	N/A
Related Policies	The University of Manchester Research Data Management Policy The University of Manchester Data Protection Policy The University of Manchester Records Management Policy The University of Manchester IT policies and guidelines The University of Manchester Intellectual Property Policy The University of Manchester Copyright Policy
Related Procedures	The University of Manchester IT policies and guidelines The University of Manchester Records Retention Schedule
Related guidance and or codes of practice:	N/A
Related Information	Open Research Statement
Policy Owner	Vice President for Research (Professor Colette Fagan); Associate Vice President for Research (Professor Chris Taylor)