Queen Margaret University
EDINBURGH

Policy Owner:	Research Data Management Working Group
Approved By:	Research Strategy Committee
Date of Issue:	February 2021
Review Period:	Annually
Last Reviewed:	N/A
Next Scheduled Review Date:	February 2022

1 Purpose

This policy aims to ensure that Queen Margaret University's research data management practices meet the highest standards.

It sets out the University's expectations so that all stakeholders recognise their responsibilities and obligations and can contribute to data being maintained and preserved as identifiable, discoverable, retrievable, and reusable assets.

The policy further:

- Supports openness and transparency in research undertaken at the University by ensuring research is of the highest integrity and is underpinned by accurate robust data
- Promotes open access to research data to facilitate data sharing and collaboration
- Ensures that the University adheres to the UK Research and Innovation Common, UKRI, principles on data policy, and provides accountability for the use of public funds
- Establishes the responsibilities of University researchers in relation to research data management and archiving.

2 Scope

This Policy applies to all University staff engaged in research. This includes staff and students, and those who are conducting research on behalf of the University.

The Policy does not apply to taught Postgraduate and undergraduate students, except where their research is included in published outputs.

3 Policy

The University recognises research data as a valuable institutional asset, and the important role of research data management in underpinning research excellence and integrity.

To this end, the University endorses the RCUK Common Principles on Data and the UK Research and Innovation Common, UKRI, principles on data policy.

Research data will be managed in line with funder requirements as well as University policy and other relevant regulations and legislation.

Research data must be:

- Accurate, complete, authentic and reliable.
- Identifiable, retrievable, and available, with as few restrictions as possible in a timely and responsible manner.
- Kept in a manner that is compliant with legal obligations, University policy and, where applicable, the requirements of funding bodies.
- Where necessary, adhere to NHS and NIHR data guidelines as a minimum

4 Data Management Plans

Clear arrangements for data management must be in place from the outset of the research project through the preparation of a **Data Management Plan**.

Data Management plans must be prepared according to funders' requirements, or elsewhere directed.

Heads of Research have overall responsibility for the effective management of research data generated within or obtained during research activities research, including by their research groups. However, it is expected that in most cases the PI of a project will be responsible for developing a DMP.

All new Data Management Plans should include processes for:

- Data capture,
- Management,
- Integrity,
- Confidentiality,
- Retention,
- Sharing and publication.

Assistance with preparing Data Management Plans and templates can be sought from the PI or found at:

DMP Online

5 Responsibilities

5.1 Principal Investigators (PI)

Assume primary responsibility for ensuring that data management activities comply with the requirements of this policy and with any relevant funders' policies.

It is their responsibility to ensure that all members of the research team with access to the research data adhere to good research data management practice

5.2 Researchers

Familiarise themselves with the requirements of this policy and with those of any funder(s) thereby assisting the PI to ensure that all data management activities are fully compliant.

Undertake any data management training provided by the University and ensure that they are aware of the guidance and support available.

5.3 The University

Ensure that appropriate training, support and advice is available to enable researchers to comply with this policy.

Provide secure and backed-up storage for data during projects and provide advice on the most appropriate repository for long-term storage of completed and/or published datasets.

Further develop services that will support data management planning and decision making on issues related to data curation and retention, disposal and open access, in partnership with the research community.

5.4 Research Data Management Working Group, RDMWG

The RDMWG will provide appropriate oversight and support for RDM principles and review and maintain any documentation relating to Research Data Management.

5.5 Research Strategy Committee, RSC

The RSC will provide overall guidance and support on all aspects of research activity within QMU

6 Personally Identifiable Data, PID

6.1 Data containing personal information, PID, must be managed in accordance with the requirements of GDPR legislation. Guidance on this can be obtained from the University Data Protection Officer.

6.2 PID should not be stored on external services, other than your QMU OneDrive account, except in exceptional circumstances and should be moved to a secure device as early as possible. See further below.

6.3 PID should not be transferred via insecure channels, such as email.

6.4 PID should be stored no longer than necessary.

6.5 Only anonymised PID may be included in an open access dataset.

6.6 Data generated via online testing platforms must be transferred onto the approved data platform as defined in the DMP as soon as the data file has been processed.

6.7 Consent forms must not be stored with data where they could compromise anonymisation.

6.8 Non-Digital PID must be stored in a secure location, such as a lockable cabinet.

6.9 If network drives cannot be used due to e.g., lack of network coverage, PID can be temporarily transferred to a University provided encrypted USB drive.

6.10 PID placed on temporary storage must be transferred back onto the network or OneDrive as soon as the requirement for temporary storage has ended.

7 Data Management Principles

7.1 Research data must be retained and disposed of securely according to the relevant retention and disposal schedule. This can be found at:

Records Retention Policy

7.2 Research data that underpins published results or is considered to have long-term value should be retained. The default period for research data retention is 10 years from date of last requested access. However, retention periods should, as a minimum, conform to the requirements of a funding agency or body.

7.3 Retained data must be deposited in an appropriate data service, or as mandated by the funder or otherwise directed.

7.4 A statement describing how and on what terms any supporting data may be accessed must be included in research outputs.

7.5 Where research is undertaken in partnership or under contract with a third party, a collaboration agreement must be signed before the start of the research that clearly addresses data ownership and partner responsibility for data storage.

7.6 Data placed on temporary storage must be transferred back onto the approved storage platform as detailed in the DMP as soon as the requirement for temporary storage has ended.

7.7 Research proposals should consider whether storage requirements may exceed those currently offered by the University. Any such potential requirement should be discussed in advance of the application with both IT and the RDM Working Group.

7.8 Before staff leave the university, data of long-term value produced using University resources must remain accessible to the University. Ownership of the data should be transferred to another member of staff on agreement of the Head of Division.

7.9 At the completion of a project, the PI must assess what data are of long-term value, and whether the data can be made openly available in a manner consistent with relevant legal, ethical and regulatory frameworks.

7.10 If research data are to be deleted or destroyed, this should be done in accordance with all legal, ethical and funder requirements and only after the written approval of the Head of Division.

7.11 Retained data suitable for external access should be stored on QMU's institutional data repository, eData unless an alternative is mandated by the funder.

Library Services manages QMU's open-access data repository, eData. It exists to preserve datasets that support research outputs published by QMU researchers, as required by funder or publisher mandates, and to maximise their sharing and reuse.

Datasets shared in eData should be used in accordance with the Terms in the QMU Repositories Policy.

7.12 After a project, a metadata record describing retained data must be made publicly available within 12 months of the project completion.

7.13 Metadata and documentation about research data should provide sufficient contextual information to enable the data to be discovered, accessed, understood, interpreted and reused by future users.

7.14 If access to the data is restricted, the published metadata should provide the reasons for the restrictions and summarise the conditions that must be satisfied for access to be granted.

7.15 All users of research datasets should acknowledge the sources of their data and abide by the terms and conditions under which they were accessed, in order to recognise the intellectual contributions of research teams and supporting organisations.

7.16 Research data must be managed throughout its lifecycle in compliance with relevant legislation.

7.17 Unless there are ethically and legally justified reasons for doing otherwise, researchers working with human subjects must ensure that they have an auditable record of each study participant's explicit informed consent. to obtain, hold and use their personal data as per research ethics guidance.

8 Cloud Storage

8.1 For the purposes of this policy, 'Cloud' storage refers to third party web-based data storage such as Microsoft OneDrive, Google Drive, Dropbox etc.

8.1 No cloud storage services should be used to store research data other than the University provided OneDrive account, unless mandated by the funder or statutory body.

8.2 Personal OneDrive accounts should not be used to store or access research data. Only accounts linked to QMU credentials should be used.

8.3 Prior to research staff leaving the employment of QMU, data stored in their OneDrive account should be transferred to an existing member of staff's account as directed by the Head of Division. This is to avoid loss of access to data.

Advice can be sought from IT if required via the Helpdesk assist@qmu.ac.uk.

8.4 Care must be taken when sharing data via OneDrive to ensure continuation of data security and privacy.

8.5 Multi Factor Authentication should be enabled for access to the OneDrive folder on any connected device. Assistance on this can be provided by the IT team via the Helpdesk, assist@qmu.ac.uk.

8 Policy Governance

This policy is owned by the Research Data Management Working Group on behalf of the Research Steering Committee.

The policy will be reviewed annually on the anniversary of its approval or in response to any legislative changes.

9 Compliance

Wilful failure to comply with this policy will be treated extremely seriously by the University and may result in disciplinary action. Failure to comply may also result in withdrawal of research funding.