UNIVERSITY OF PLYMOUTH

Research Data Policy

Owner:	University Research Ethics & Integrity Committee (UREIC)
Author:	Information and Data Management Advisory Group (IDMAG)
Date:	01/06/2018
Security Level:	**PUBLIC**
Status:	Published
Version:	1.0
Reference:	
Document Link:	
Review Date:	01/06/2020

Research Data Policy

Contents

Version	Contributors	Details	Date	Approved by	Date
0.1	Jason Harper (Content Strategy Manager) and Elena Menendez-Alonso (Research Repository & Curation Manager)	Initial draft	17/02/2017	-	-
0.2	JLH and EMA	Revised draft	15/03/2017	-	-
0.3	Review by John Martin (Head of Research Support and Development)	Added note to clarify the definition of 'student' in the context of the policy	10/04/2017	-	-
0.4	Review by RDSS project team	Moved 'Principles' to section 1. Merged committees and roles. Added 'DMP reviewer' role. Added Figure 1 (lifecycle)	18/05/2017	-	-
0.5	EMA	Added principles graphic to tie in with guidance	04/08/2017	-	-
0.6	EMA	Updated logo and colours	23/11/2017		
0.7	EMA	UREIC review	08/01/2018		
0.8	Klara Łucznik (Research Administrator) and EMA	Update to align with new Research Ethics policy	02/02/2018		
0.9	JM, KL, JH, EMA	Incorporate ISC levels (section 3.2)	01/03/2018		
0.10	Professor Roberta Mock (Director of the Doctoral College) and EMA	Follow up from R&I Committee review. Update to clarify expectations on PG Research students	11/04/2018		
1.0	EMA	Updated version to 1.0 (published). Removed "draft" watermarks	01/06/2018	Professor Jerry Roberts (DVC Research & Enterprise)	01/06/2018

1. Introduction

1.1 The University of Plymouth recognises that **good practice in research data management and open access to research data are integral to high-quality research**. They protect intellectual and financial investment, support reliable verification of results, and enable additional innovative research.

1.2 **Principles:**

To facilitate good practice in Research Data Management (RDM) and encourage open access to research data, the University establishes the following principles:

1. Data management planning is embedded in research activities throughout the lifecycle of every project.
2. Research data management practices are compliant with legal, ethical, contractual and funding requirements.
3. Data is well organised and documented from the outset to ensure its integrity, discovery and reusability.
4. Data is stored securely and protected against unauthorised modification or destruction.
5. Data of long-term value is selected for preservation.
6. Researchers recognise the value of research data to the wider community and are committed to making their data open access and usable, *wherever possible* and within an appropriate and defined period.

1.3 **Purpose:**

The purpose of this policy is to make University of Plymouth researchers aware of their responsibility to exercise **good practice in RDM**; and to ensure that their **research data is made openly available for use by others wherever possible**, in a manner consistent with relevant legal, ethical, disciplinary and regulatory frameworks. Adherence to the policy will demonstrate their commitment to research funder mandates, the RCUK Concordat on Open Research Data[1], the *Code of Good Research Practice,* and the *Research Ethics Policy*[2]. The **aims** of the policy are:

1. To set standards of practice for developing a consistent approach to RDM and open data sharing across the University of Plymouth;
2. To ensure that research data is stored, organised, documented, preserved and shared in accordance to its value and to legal, ethical, contractual and funding requirements;
3. To define roles and responsibilities for the governance of research data;

[1] HEFCE, et al. (2016). *Concordat on Open Research Data*. RCUK. Available from: http://www.rcuk.ac.uk/documents/documents/concordatonopenresearchdata-pdf/ (accessed 8th January 2017); and, *RCUK Common Principles on Data Policy* (July 2015). Available from: http://www.rcuk.ac.uk/research/datapolicy/ (accessed 8th January 2017)

[2] University of Plymouth (2018). *Research Ethics Policy & Code of Good Research Practice*. Available from: https://www.plymouth.ac.uk/research/governance (accessed 26th February 2018)

4. To ensure that data management plans are developed for each research proposal that requires the collection or generation of data, and that additional requirements, roles and responsibilities are documented in the plans.

1.4 **Audience:**

This policy applies to University researchers (staff or postgraduate research students[3]) that have responsibility for any aspect of research data creation, collection, use, maintenance or disposal.

1.5 **Scope:**

The policy applies to all research data generated by University of Plymouth researchers, or under the auspices of the University as stated in the *Code of Good Research Practice*, and the *Research Ethics Policy*. In cases when research is funded by a third party, any agreements made with that party concerning intellectual property rights, access rights and the storage of research data take precedence over this policy.

2. Roles and responsibilities

2.1 The roles and responsibilities for RDM align with those stated in the *'Information Governance Roles & Responsibilities'* document[4]. Figure 1 provides an overview of the roles, responsibilities and support infrastructure in the context of the research lifecycle.

2.2	**Deputy Vice Chancellor for Research**	Fulfils the role of *Senior Research Data Owner* (SRDO) with overall accountability for research data.
2.3	**University Research Ethics & Integrity Committee (UREIC)**	Chaired by the **Deputy Vice Chancellor for Research**; it is the owner of this policy and has overall responsibility for mandating adherence to it and ensuring the availability of resources to support its implementation. Responsible for: 1. Ensuring that RDM measures and procedures are in place to protect against risk. 2. Monitoring and reviewing compliance with this policy.
2.4	**Faculty Research Ethics & Integrity Committee (FREIC)**	The **Chairs of FREIC** fulfil the role of *Data Asset Owners* which makes them accountable for the data assets generated by their Faculty. Each FREIC is responsible for: 1. Ensuring that data management plans (DMP) have been completed and peer reviewed, before work on a project starts and, if relevant, before granting ethical approval for the proposed research. 2. Producing monitoring reports for the *University Research Ethics & Integrity Committee.*

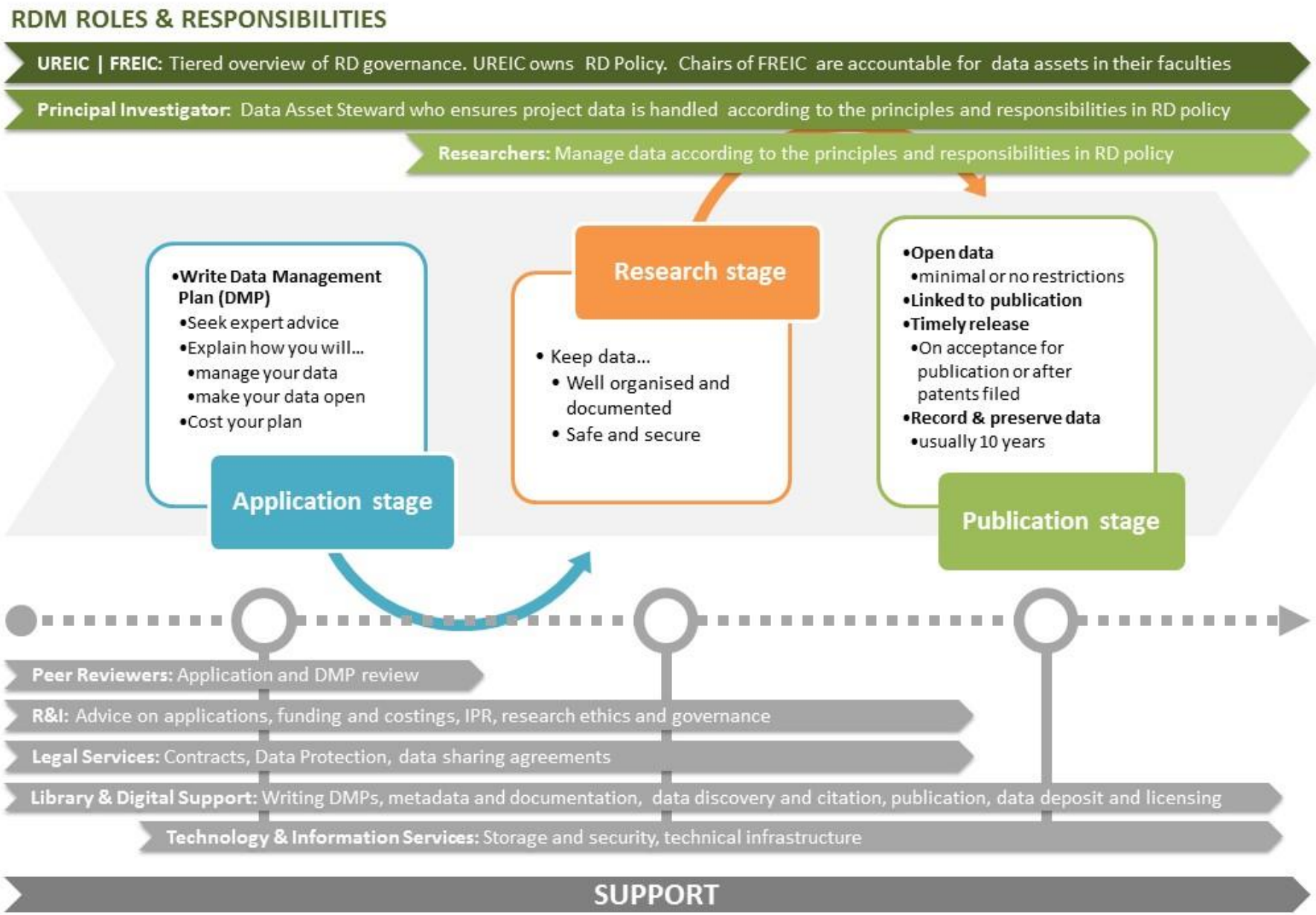
[3] In the context of this policy, 'student' refers to 'Postgraduate Research Student'. In most taught programmes, whether undergraduate or postgraduate projects, the student, not the institution, owns data. Nonetheless, tutors are expected to encourage students to adopt best practice in data management. Valuable research data generated by undergraduate students should be flagged by tutors, and if the student gives their consent, it could be archived for preservation and reuse.

[4] University of Plymouth (2017). *Information Governance*. Available from: https://www.plymouth.ac.uk/your-university/governance/information-governance (accessed 7th February 2017)

		3. Identifying training requirements and providing professional development opportunities for researchers relevant to domain specific data management practice.
2.5	**DMP Peer Reviewers**	Responsible for peer reviewing data management plans (DMP) and providing feedback to fellow researchers to help them improve their data management practice in alignment with this policy.
2.6	**Principal Investigators (PI)**[5]	Fulfil the role of *Data Asset Steward*, and are accountable for ensuring that: 1. Good practice is implemented by all researchers involved in a project. 2. Data is handled appropriately according to University policies, and legal, ethical, regulatory and contractual requirements. 3. A DMP is completed and peer reviewed prior to grant application and the project commencing. 4. The DMP is reviewed and updated throughout the project. 5. Data is deposited in accordance with section 3 of this policy.
2.7	**Researchers**	Responsible for making themselves aware of and adhering to relevant legislation and regulation, funders' expectations and the requirements stated in section 3 of this policy.
2.8	**Research & Innovation, supported by Library & Digital Support**	Responsible for: 1. Defining the core University offering in support of research data management and communicating that to researchers. 2. Providing central guidance and training to support generic good practice in data management and open data deposit. 3. The *Funding Advisory Service* is responsible for providing **cost modelling guidance** to *Principal Investigators* at the start of the data management planning process.
2.9	**Technology & Information Services**	Responsible for the **provision and maintenance of core infrastructure** to support RDM and the open deposit and long-term preservation of research data.

[5] For collaborative external grant projects, the lead University of Plymouth Researcher will assume this role.

Figure 1. RDM roles, responsibilities and support through the research lifecycle



3. Requirements

This section outlines the actions which researchers are required to carry out in order to follow the principles stated in 1.2. By fulfilling these requirements, researchers will also ensure commitment to research funder mandates and the RCUK Concordat on Open Research Data.

3.1 Data management planning

1. The PI ensures that a *data management plan (DMP)* is completed for each new research proposal.
2. If the funder requires a DMP, the plan should be prepared according to the funder's requirements. Otherwise, the DMP should outline explicitly how the researchers will address the requirements in sections 3.2 to 3.6[6].
3. The DMP should also explicitly identify:
    1. Responsibilities for data management throughout the project, including who will be the *data asset steward* once the data is archived.
    2. The costs of data management throughout the project, including storage, analysis, and preparation for deposit[7]. Where permitted by the funder, these costs should be recovered through the research grant, supporting the University's strategic principle of increasing the financial sustainability of research[8].
    3. Provisions made for open data sharing at the end of the project, unless there are valid and justifiable exceptions to this principle (see section 3.2).
4. The University does not provide central storage for physical items. If physical data has long-term value or underpins published research, researchers should include the costs of digitising it in their funding applications. Digital data can then be deposited in the University repository or an *external data repository*.
5. The DMP is a living document that will be used as a point of reference throughout the project and edited to capture new requirements and decisions.
6. The PI deposits the final copy of the DMP in the research repository.

3.2 Ethical and legal compliance

1. Research data is created, managed and shared in a manner that is compliant with:
    1. The University's *Code of Good Research Practice*, and the *Research Ethics Policy.*
    2. Legal and contractual obligations for particular types of research: among others, research involving human participants, human tissue and animals.
    3. Requirements of funding bodies.
    4. Project-specific protocols approved by the University's Research Ethics and Integrity Committee.
    5. The *Information Security Classification Policy*[9].

---

[6] See RDM online guide (http://plymouth.libguides.com/rdm) for templates and guidance on preparing DMPs.

[7] Guidance can be obtained from the *Funding Advisory Service*.

[8] University of Plymouth (2016). *Advancing Knowledge, Transforming Lives. Strategy 2016-2020*; and *Research and Innovation Strategy 2017-22*.

[9] University of Plymouth (2017). *Information Security Classification Policy*. Available from: https://www.plymouth.ac.uk/your-university/governance/information-governance/information-security (accessed 7th February 2017).

2. Intellectual property (IP) rights over research data are considered from the start of the project. This involves:
    1. Determining IP rights in accordance with the University's *Intellectual Property Policy*[10];
    2. Respecting the IP rights of others when using third party data for research;
    3. Considering how rights given to third parties will impact on the researcher's ability to share data at the end of the project.
3. It is the responsibility of PIs (or their nominated delegates) to assign security classification levels to all datasets in line with the *Information Security Classification Policy*.
    1. The security classification levels for research data are:

    Level 1 - Restricted: Disclosure would cause severe harm to individuals or the University.

    - Data from medical research with human participants (e.g., human tissue or data, clinical trials data).
    - Data defined under the Data Protection Act 1998 (DPA)[11] as 'sensitive personal data' (such as individually identifiable ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health conditions, sexual orientation, and criminal record) for which consent to release has not been obtained.
    - Data restricted by contract or confidentiality agreement.
    - Commercially sensitive data.
    - Draft research findings on controversial topics or of significant value.
    - Account passwords that can be used to access confidential information.

    Level 2 - Confidential: Disclosure could cause harm to individuals or the University.

    - Data defined under the DPA as 'personal data'[11] (e.g. information or a combination of data that identifies living individuals, such as home / work address, age, phone number, photographs) and for which consent to release has not been obtained.
    - Consent forms for participation in research involving human participants.
    - Patent applications.
    - Drafts of research papers and reports, and their underlying data not in Level 1.

    Level 3 - Standard: Disclosure would not cause harm, but the researcher has chosen not to release.

    - Any research data not cleared for publication, including anonymised data from research with human participants.
    - Finalised research papers and reports, and their underlying data cleared for publication (see below) but deposited under embargo.
    - Other data and documentation (not in Level 1 or 2) with no value to external users.

    Level 4 - Public (or open): The data is openly available to the public.

    - Data underpinning publications or of long-term value that has been cleared for publication by meeting defined pre-conditions, e.g.: personal data has been anonymised, participants have given explicit consent for publication and the researcher owns the rights or has been given permission to publish by the rights-holder(s).
    - Research publications and data that are already in the public domain.

    2. The classification level should be assigned as soon as possible in the project, and no later than the point at which the data is created or received from a third party.

[10] University of Plymouth (2017). *Intellectual Property*. Available from: https://www.plymouth.ac.uk/research/support/intellectual-property (accessed 7th February 2017)

[11] Information Commissioner's Office (2018). *Key definitions of the Data Protection Act*. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/ (accessed 27th February 2018)

4. It is the responsibility of the researcher to consider how legal and ethical restrictions will impact on their ability to share data at the end of the project and address these considerations in their DMP.
    1. Researchers should plan and take action, as early as possible, to ensure that data can be shared in keeping with funder mandates[12]. Action could include anonymisation, adding explicit clauses on data sharing to consent forms, or gaining approval from third parties for data to be published after a suitable embargo (for details, see Section 3.6).
    2. The security classification level should be reviewed during the lifecycle of the project, as different versions of the dataset are created, and to reflect changes in preparation for publication (e.g., anonymisation), as well as usage conditions set by rights-holders or participants.

3.3 Organisation, documentation and metadata

1. Research data is created and maintained following the data quality standards set in the University's *Data Quality Policy*[13]: research data should be accurate, valid, reliable, relevant and complete.
2. Research data is organised and documented to ensure its future discovery and reusability.
3. Consideration is given to the use of open or widely available file-formats and metadata standards that will facilitate the discovery, interpretation and reusability of the data.

3.4 Storage and backup

1. Researchers ensure that data is stored in a secure location and managed in accordance with the University's *Information Security Classification Policy* and any additional ethical, legal, contractual and funder requirements.
2. Access to data during the research phase is controlled as outlined by the *Information Security Classification Policy* to guarantee the security and integrity of the data.
3. There is a back-up schedule in place that meets the requirements set by the *Information Security Classification Policy*.

3.5 Retention, preservation and disposal

1. Research data that supports published research findings or is of long-term value is retained for a minimum of 10 years from collection or creation of the data or publication of the research results (whichever is the latter).
2. Research data is retained for longer than 10 years where an increased retention period is required to meet legal, statutory, contractual or funder requirements.
3. A *record of the data*[14] is added to the University research repository to enable the discovery and identification of the dataset. The record will consist of:
    1. Structured metadata describing the dataset (e.g., author, project, funder, description of the data).

---

[12] The Concordat on Open Research Data recognises that "*not all research data can be open and [...] that access may need to be managed in order to maintain confidentiality, guard against unreasonable cost, protect individuals' privacy, respect consent terms, as well as managing security or other risks*". However, "*any restrictions must be justified and justifiable*".

[13] See University of Plymouth's *Information Governance* page

[14] See RDM online guide (http://plymouth.libguides.com/rdm) for guidance on creating a data record.

2. Details of how to access the data (e.g., a DOI or URI link if the data is openly available; otherwise, the contact details of the data asset steward).
3. If access to the data is restricted, a statement that justifies the decision, and the nature of any restrictions.

4. Datasets can be deposited in the University repository, by uploading them as an attachment to the record. Access to the dataset can be set as open (see section 3.6) or restricted. Any conditions of access should be proportionate, and not unduly restrictive. Dataset deposit should be compliant with ethical, legal, contractual and funder requirements (see section 3.2).
5. Publications should include a *data access statement* linking to the *data record* to enable readers to discover the dataset and explaining how it can be accessed.
6. Upon disposal of the data at the end of its retention period, the data record should be amended to indicate that the data has been destroyed and the reason for the disposal.
7. The disposal and destruction of research data is undertaken in accordance with the University's *Information Security Classification Policy* and *Records Retention Schedule*[15], as well as any additional requirements established by funders and third-party rights holders.

3.6 Sharing and publishing

1. Research data that supports published research findings or is of long-term value is considered for open deposit.
    1. Research data sharing or publishing is undertaken in accordance with the University's *Information Security Classification Policy* and any additional ethical, legal, contractual and funder requirements (see section 3.2). This will involve ensuring that: a) the data is complete and relevant; b) consent to archive, share or publish the data has been obtained from rights holder and participants; and c) the data has been suitably documented and prepared for publication, e.g., by anonymising personal information[16].
    2. Subject to 3.6.1.1, data is made accessible and reusable (by the publication date if it supports published findings), and in citable form.
    3. It is acceptable to set up an embargo to allow for reasonable first use of the data. However, any embargo must be for an appropriate and well-defined period.
2. The data can be deposited in the University repository, or a recognised *external data repository*.
3. Each deposited dataset includes:
    1. Documentation to enable the interpretation and reuse of the data.
    2. The terms of access and reuse. For publicly funded research, it is expected that the dataset will be assigned a *Creative Commons* license, which is as open as possible.
    3. Instructions on how to cite the data.
    4. The DMP.
4. If the dataset has been deposited in an external repository, a *record of the data* is added to the research repository (as described in section 3.5.3) to enable the discovery of the dataset.

---

[15] University of Plymouth (2017). *Records Management*. Available from: https://www.plymouth.ac.uk/your-university/governance/information-governance/records-management (accessed 7th February 2017).

[16] The practice of anonymisation should comply with professional standards of research discipline. Relevant techniques are presented at: Information Commissioner's Office (2012) *Anonymisation code of practice*. Available from: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

4. Research information management systems

4.1 The University's research information management systems include:

1. **Symplectic Elements** is the University's Current Research Information System (CRIS). Researchers use Elements to create data records and deposit datasets.
    1. Elements populates publication profiles on the University website.
    2. Elements sends records and data files to the repository, PEARL.
2. **PEARL** is the University's research repository, and the institution's publicly accessible catalogue of research datasets and publications.

4.2 The research information management systems support the implementation of this policy by:

1. Providing evidence of research datasets deposited in compliance with open access expectations to:
    1. Satisfy funder reporting requirements.
    2. Inform Faculties, Schools and Research Institutes.
    3. Benchmark against other UKHEIs.
2. Enabling wider discovery of University of Plymouth research datasets for harvesting by other databases or repositories, and for re-use.

5. Related policies

5.1 Data Protection Policy

5.2 Data Quality Policy

5.3 Information Governance Roles & Responsibilities

5.4 Information Security Classification Policy

5.5 Information Security Policies

5.6 Intellectual Property Policy

5.7 Records Retention Schedule

5.8 Research Ethics Policy – includes 'Code of Good Research Practice'

5.9 Research Publications and Open Access Policy

6. Further support and guidance

6.1 Additional information can be found via the University's Research Support website and the RDM online guide.

Appendix: Glossary

Data Access Statement	Information added to a research publication to describe the dataset(s) that the research is based upon, and to link to a *data record* which provides additional details about the data and how to access it[17].
Data asset	In the context of this policy, a valuable dataset.
Data Asset Owner	Senior individual who has overall accountability for the data assets produced through that department's research activities, and for ensuring that the value and sensitivity of the data assets have been recognised, and that they are handled and managed accordingly against any risk. See the University's policy on *Information Governance Roles and Responsibilities*.
Data Asset Steward	Individual with day-to-day operational responsibility for the management of a data asset. In the context of this policy, *Principal Investigators* or lead researchers.
Data management plan (DMP)	A tool for demonstrating to a funder and the University that the Principal Investigator of a research project has adequately considered and made provision for the data management needs and costs of their project, including responsibilities regarding data collection and quality, the application of data processing standards, appropriate data protection and security, and data sharing. A DMP should be used as a practical planning tool to aid the management of data throughout the project. It is a living document and should be referred to and reviewed regularly.
Data record	Structured *metadata* which describes a dataset in its context. Effectively a catalogue record which needs to be created and deposited in the University repository in order to describe the dataset, make it discoverable, and enable others to reuse it. It can be accompanied by files containing the actual data, and by documentation enabling the interpretation of the data.
Dataset	In the context of this policy, a *selection* of the data which has been collected during the period of a research project, chosen for preservation and sharing because it supports published research findings or is of long term value.
Deposit	The act of creating a *data record*, and uploading any related dataset files or documentation, to the University repository, or an external data repository.
Disposal	The act of destroying data at the end of its retention period. Disposal must be undertaken in accordance with the security classification level of the data (see section 3.2).
Embargo	The period during which access to the dataset is temporarily restricted. Usually, embargoes are applied while researchers are awaiting publication or pursuing a patent. Typical embargo periods range from 6 to 24 months.
External data repository	An approved (often discipline specific) national, European or international repository for the deposit and preservation of datasets.
Metadata	Data that provides information about other data, e.g., title, author, description, etc.
Open research data	Research data that can be freely accessed, used, modified, and shared, provided that there is appropriate acknowledgement, if required[1].
Preservation	The actions required to ensure that data of long-term value remains accessible and usable.

[17] See RDM online guide (http://plymouth.libguides.com/rdm) for examples of data statements (https://goo.gl/VgmvaP).

Record of the data	See Data Record
Research data	Any material created or collected that is necessary to generate, support and validate original research results, observations, findings or outputs, irrespective of the format or the media in which they may exist.
Research data management (RDM)	A range of activities related to the creation, collection, processing, maintenance, storage, disposal, sharing and publishing of research data in a way which facilitates its most appropriate, efficient and effective use and is compliant with legal obligations.
Researcher	All research-active members of the University including employees and postgraduate research students. Persons not directly affiliated with the University, but who, for purposes of research, make use of or are physically present at the institution, are also included in the term. Visiting researchers or collaborators may also be expected to comply with the policy.
Retention	The agreed period of time the dataset will be retained for, prior to its disposal.
Retention Schedule	A list of record types stating how long they must be kept for, prior to their disposal. The schedule also defines which area of the University is responsible for the storage and disposal of records and what security classification applies to a record and determines how it should be stored or destroyed.
Senior Research Data Officer (SRDO)	Senior executive with overall responsibility for data as a strategic asset of the University, ensuring that the value to the organisation is understood and recognised, and that measures are in place to protect against risk.
Storage and backup	Requirements that must be addressed in a DMP to ensure that data collected during the project is safeguarded and available throughout the project and for deposit at project end. The storage and backup options available may be subject to factors such as the data volume, and the security classification of the data. The University's Information Security Classification Policy provides guidance on the technical and security standards required for the storage of confidential and sensitive data.