

Guidance for the Implementation of the University of Aberdeen's Research Data Management Policy

The guidance below is provided to further support research staff in implementing the above policy.

Principal Investigator Responsibilities

The Principal Investigator (PI) is responsible for adherence to the RDM Policy and:

1 Compliance

- 1.1 Ensuring compliance with the University Policy on Data Protection which complies fully with the General Data Protection Regulation ((EU) 2016/679) and the UK Data Protection Act 2018, or any successive regulation or legislation.
- 1.2 Research data management practice – see Research Data Management Policy for definition.
- 1.3 Recording data management decisions and ensuring their availability for audit purposes.
- 1.4 Ensuring data management practice is carried out in accordance with participant consent.
- 1.5 Ensuring all users (including third parties), who have access to University-owned devices comply with the UoA Data Protection Policy, Information Security Policy, sub-policies, and IT Conditions of Use.
- 1.6 Ensuring transfer or transportation of data, particularly personal, confidential, and commercially-sensitive data, is carried out in accordance with Data Protection legislation, the University of Aberdeen Data Protection Policy, and using approved University transfer mechanisms (e.g. secure file transfer protocols such as Zend.to).

2 Risk Assessment

- 2.1 Assessing and managing risk according to the nature of the research project, its potential to create harm, potential risk to the University's reputation, and financial risk.
- 2.2 To consider all relevant risks and ensure, where possible, mitigations are built into the project design. If not possible, ensuring significant risks are understood and accepted by Head of School.
- 2.3 Where relevant (where research involves personal data), the [Data Protection Impact Assessment screening questions](#) should be undertaken to assess risk and, where necessary, a full DPIA should be completed.
- 2.4 In advance of any data sharing, and where no other formal university processes provide the necessary assurance, carry out an [Information Sharing Risk Assessment \(ISRA\)](#) for each organisation data is to be shared with. Risk assessment must be included in circumstances where data is to be:
 - Collected by a third party on behalf of the University (e.g. a supplier, partner, or cloud service);
 - Shared with a third-party collaborator outside the UK, either through access to UoA infrastructure or by transfer;
 - Shared with a supplier, either through access to UoA infrastructure or by transfer;
 - Hosted by a third party (e.g. a cloud service).
- 2.5 Where a University research project involves working with partners outside the UK, risk assessment may need to consider the legislative framework of the relevant country/countries.
- 2.6 Where University-owned devices are to be used by third parties to collect, store, or transfer data, ensuring the device set up is discussed with DDIS (Digital and Information Services) and, where data governance issues or risks are identified, enabling appropriate device management to be put in place.

See Annex 1 for further guidance/process for managing risk.

3 Data Management

- 3.1 Managing research data in line with all relevant UoA Policies and guidelines.
- 3.2 Identifying and managing who has access to the data throughout the lifetime of the project, and specifying appropriate levels of access to the data (e.g. Read Only or Read/Write).
- 3.3 Ensuring data collection (regardless of methodology e.g. surveys, questionnaires, interviews etc.) is undertaken using University approved data collection mechanisms and is carried out with the necessary institutional consent, approvals, and data protection in place.
- 3.4 If leaving the organisation, identifying and agreeing the new data custodian.
- 3.5 Consulting relevant third parties in relevant aspects of data management (e.g. research participants; academic and non-academic partners) in making these decisions.

4 Data Management Plans (DMP)

- 4.1 DMPs are required, pre delivery phase, for all research projects where any of the following apply:
 - The funder mandates the completion of a DMP;
 - Relevant ethics review board determines requirement for a DMP;
 - Following review of project design and risk, the PI is advised by any of: the Information Governance Team (which includes the Data Protection Officer), the IT Security Manager, Business Development Officer, Information Champion, or Directorate of Digital & Information Services Digital Research Team.
- 4.2 DMPs will take account of requirement for public access to research data under appropriate safeguards or legitimate restrictions, specified on ethical, legal, or regulatory grounds, or on commercial conditions of funding.
- 4.3 Where a third party or partner organisation is responsible for the compilation of the DMP, the University of Aberdeen upholds the right to negotiate the terms of this document to ensure our institutional practices are reflected and honoured, led by the PI in the first instance.
- 4.4 Where risks are identified or a DMP is explicitly mandated (see Research Data Management Policy for further guidance), projects should include a DMP up-front as an integral part of a research proposal:
 - DMPs should be kept up to date for the lifetime of the project and reflect any changes in practice to the existing plan, e.g. the way data is to be managed, accessed, shared, protected, or stored;
 - The length of time data is to be retained and the related parameters should be set out in the DMP;
 - DMPs will consider appropriate access to research data under appropriate safeguards or legitimate restrictions, specified on ethical, legal or regulatory grounds, or on commercial conditions of funding;
 - DMPs should indicate where data is/will be deposited (e.g. UoA storage facility or outside the University, for example, in a disciplinary or national data repository).

5 Open Access and Preservation

- 5.1 Supporting and responding appropriately to the University's aims in respect of open access publishing of data.
- 5.2 Assessing and identifying longer term storage and open access opportunities, and ensuring these are costed appropriately in funding applications.
- 5.3 Ensuring that intellectual property rights are retained in line with University, funder, data supplier, and third-party requirements and rights.
- 5.4 Researchers should identify the most appropriate repository based on relevant legislation, polices, contractual obligations and consent obtained from research participants.
- 5.5 Options for consideration include:
 - 5.5.1 National Archives
 - 5.5.2 Funder Repositories

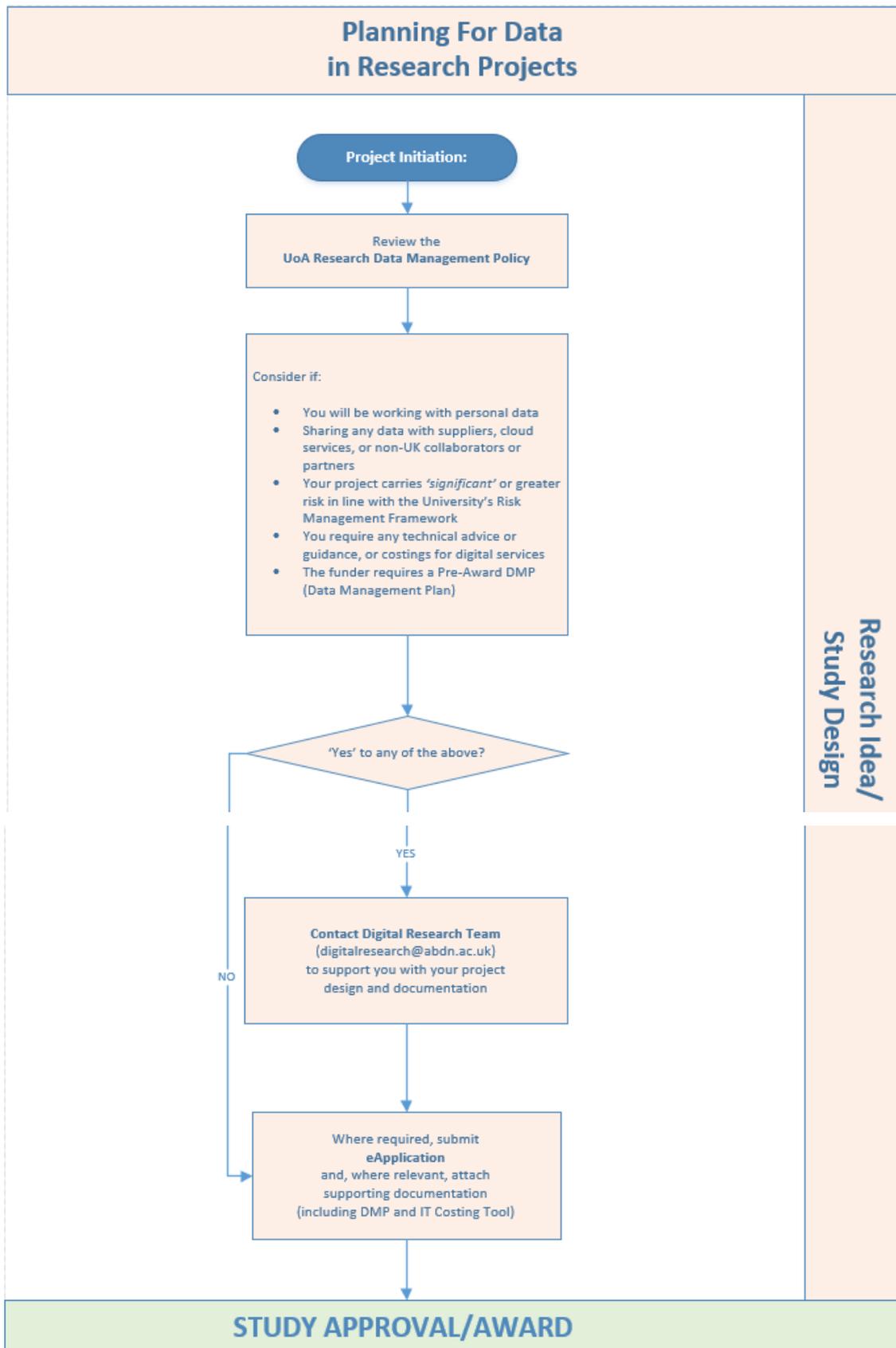
- 5.5.3 Discipline Specific Repositories
- 5.5.4 Other External Repositories
- 5.5.5 AURA
- 5.5.6 Data Catalogue (PURE)
- 5.5.7 Other UoA Managed Storage (for consideration where none of the above are deemed appropriate)
- 5.6 All data sets should be listed in PURE with relevant metadata, data location, and where applicable the DOI listed.

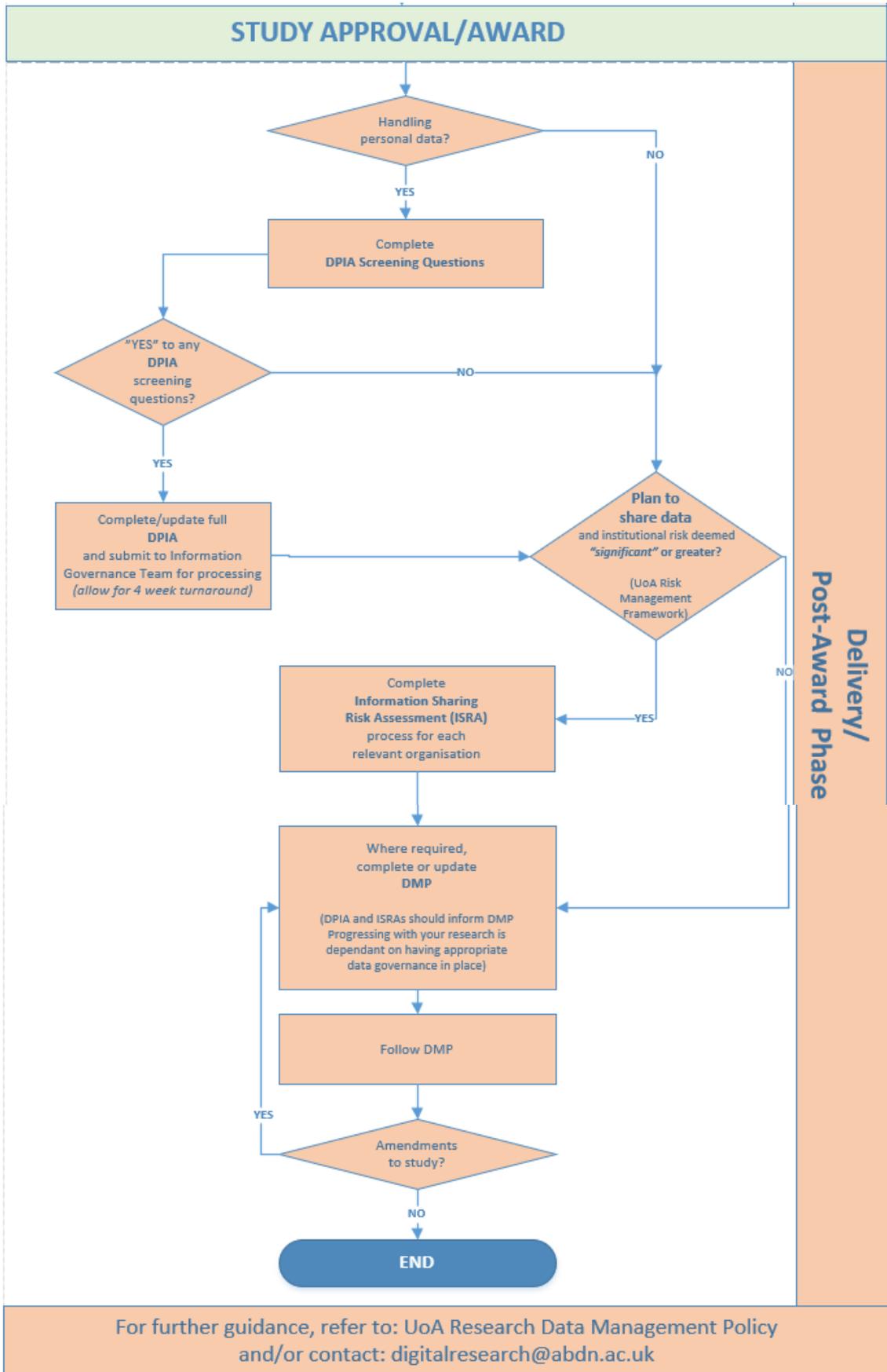
For further information or support, please contact digitalresearch@abdn.ac.uk

Revision History:

Version	Date	Reason for release/Status
1.0	3 April 2020	Published copy

Guidance on Process:





Title	Research Data Management Guidance Note
Author / Creator	Gail Smillie & Dawn Foster
Owner	Elizabeth Rattray
Date published / approved	16 April 2020
Version	2
Date for Next Review	April 2022
Audience	Research staff and students
Related	
Subject / Description	University guidance note on Research Data Management
Equality Impact Assessment	Not applicable (there are no equality issues arising from the application of this policy or guidance note)
Section	Research & Innovation
Theme	Research Data Management
Keywords	Research, research data, data management, data storage, data retention, retention period