UHI RDM policy references and appendices

The UHI RDM policy and guidelines were developed during 2016/17 by a working group comprised of:

Stuart Knight	Research Information Systems Officer
Ruth Priest	University Librarian
Philippa Currie	Records Archivist Records Manager
John Maher	Director of LIS
Steve Gontarek	Head of ICT, SAMS
John Alexander Smith	Head of Integrated Technologies, LIS
Michael Rayner	Dean of Research
Robert Polson	Librarian, CfHS

With reference to:

Darryl Thompson	Operations Manager, LIS
Sarah Wright	Grants and Contracts Officer
Karen Furness	Grants and Contracts Manager
Neil Simco	Vice Principal Research and Impact
Melanie Smith	Head of Research Development, IC
Lucio Marcello	Researcher, RLI (IC)
Donald Maclean	College Librarian, Perth
Roger Sendall	Head of Governance and Records Management
Suzanne Stewart	Information Development Manager, IC

The UHI Research Data Management Policy and Guidance document has been written to include the principals set out in the following regulatory and advisory documents:

Appendix A – Regulatory documents

Overarching guiding policy

Concordat on Open Research Data (UUK, HEFCE, RCUK, Wellcome Trust, July 2016) – **Appendix B**
RCUK Common Principles on Data Policy (RCUK, July 2015) – **Appendix C**

Discipline/funder specific policies

ESPRC Expectations on Research Data Management (ESPRC, October 2014)
ESRC-DFID Example Data Management Plan (ESRC , August 2015)
MRC Policy on Open Research Data (MRC, October 2016)
NERC Data Policy (NERC, March 2014)
AHRC (adopts 'RCUK Common Principles on Data Policy')
BBSRC Data Sharing policy Statement (BBSRC, March 2016)
STFC (adopts the Data management plan guidance provided by the Digital Curation Centre)

Browse funders websites for the appropriate document for the specific requirements of the funding body funding your research should always be made: Search "data management" on the websites of each council for their current requirements.

Appendix B - Principals of open research data

Developed jointly by UUK, HEFCE, RCUK, Wellcome Trust, this document is intended as a guide to developing best practise in open research data management.

According to the 'Concordat on Open Research Data' (July 2016) university policy must be guided by the following principals:

Principle #1
Open access to research data is an enabler of high quality research, a facilitator of innovation and safeguards good research practice.

Principle #2
There are sound reasons why the openness of research data may need to be restricted but any restrictions must be justified and justifiable.

Principle #3
Open access to research data carries a significant cost, which should be respected by all parties.

Principle #4
The right of the creators of research data to reasonable first use is recognised.

Principle #5
Use of others' data should always conform to legal, ethical and regulatory frameworks including appropriate acknowledgement.

Principle #6
Good data management is fundamental to all stages of the research process and should be established at the outset.

Principle #7
Data curation is vital to make data useful for others and for long-term preservation of data

Principle #8
Data supporting publications should be accessible by the publication date and should be in a citeable form.

Principle #9
Support for the development of appropriate data skills is recognised as a responsibility for all stakeholders.

Principle #10
Regular reviews of progress towards open research data should be undertaken.

Appendix C – RCUK suggested best practice principals

RCUK have produced their own guide to the overarching principals the discipline Research Councils are expected to adhere to when forming their own policy. These are reproduced here for quick reference but the document in full is available as the document **RCUK Common Principles on Data Policy**.

Principle #1
Publicly funded research data are a public good, produced in the public interest, which should be made openly available with as few restrictions aspossible in a timely and responsible manner.

Principle #2
Institutional and project specific data management policies and plans should be in accordance with relevant standards and community best practice. Data with acknowledged long-term value should be preserved and remain accessible and usable for future research.

Principle #3
To enable research data to be discoverable and effectively re-used by others, sufficient metadata should be recorded and made openly available to enable other researchers to understand the research and re-use potential of the data. Published results should always include information on how to access the supporting data.

Principle #4
RCUK recognises that there are legal, ethical and commercial constraints on release of research data. To ensure that the research process is not damaged by inappropriate release of data, research organisation policies and practices should ensure that these are considered at all stages in the research process.

Principle #5
To ensure that research teams get appropriate recognition for the effort involved in collecting and analysing data, those who undertake Research Council funded work may be entitled to a limited period of privileged use of the data they have collected to enable them to publish the results of their research. The length of this period varies by research discipline and, where appropriate, is discussed further in the published policies of individual Research Councils.

Principle #6
In order to recognise the intellectual contributions of researchers who generate, preserve and share key research datasets, all users of research data should acknowledge the sources of their data and abide by the terms and conditions under which they are accessed.

Principle #7
It is appropriate to use public funds to support the management and sharing of publicly-funded research data. To maximise the research benefit which can be gained from limited budgets, the mechanisms for these activities should be both efficient and cost-effective in the use of public funds.

Appendix D - Funding application data checklist

The elements in the below table should be considered and costed for every funding application.

Confirm you have considered the following points, and added provision where necessary within your funding application costing:

COST	Yes, No, N/A
Data Management	
Website, Web hosting, server space	
Research Data Storage	
IT Hardware – if a large amount of data storage will be required build-in to your application the cost of hard drives/servers/archive space	
GIS Storage – can generate a requirement for a large amount of storage space	
Maps, charts etc.	
Software licenses	
Publishing licences – is there a requirement from a funder, Research Council or Department to publish any articles or results 'Gold' open access that may incur any Article Processing Charge (APC)?	

Appendix E - MEDIN standards

As MEDIN metadata standards (for Marine Sciences data deposits) are evolving at an international level and are therefore subject to change, it is recommended you access the most current definition of the standard from: http://www.oceannet.org/marine_data_standards/medin_disc_stnd.html

For reference, as of April 2017, there were 30 defined elements required to deposit data to MEDIN standards in a mixture of mandatory, optional or conditional fields (P denotes fully available in PURE). These are listed below but a full explanation of the elements is at the URL above.

1 - Resource title (M) P
2 - Alternative resource title (O)
3 - Resource abstract (M) P
4 - Resource type (M) P
5 - Resource locator (C) P
6 - Unique resource identifier (M) P
7 - Coupled resource (C) P
8 - Resource language (C)
9 - Topic category (C)
10 - Spatial data service type (C) P
11 - Keywords (M)
12 - Geographic bounding box (C) P (partial – geospacial point)
13 - Extent (O)
14 - Vertical extent information (O)
15 - Spatial reference system (M)
16 - Temporal reference (M) P
17 - Lineage (C)
18 - Spatial resolution (C)
19 - Additional information source (O) P
20 - Limitations on public access (M) P
21 - Conditions applying for access and use (M) P
22 - Responsible party (M) P
23 - Data format (O)
24 - Frequency of update (C)
25 - Conformity (C)
26 - Metadata date (M)
27 - Metadata standard name (M)
28 - Metadata standard version (M)
29 - Metadata language (M)
30 – Parent ID (O)

Appendix F – Mendeley Data Service

*Full information on this service available at **Mendeley Data**.*

Some FAQ's about the service from Mendeley:

What is Mendeley Data?

Mendeley Data is a place where individual researchers can upload and share their research data for free. However, it should be noted that although free currently this could change at any time. Datasets can be shared privately amongst individuals, as well as published to share with the world. Sharing research data is great for science as it enables data reuse and supports reproducibility of studies. It's also a fantastic way to gain exposure for your research outputs, as every dataset has a DOI and can be cited.

What does it mean for a dataset to have a DOI?

A digital object identifier (DOI) is an alphanumeric code providing a unique and persistent link to specific electronically published content.

Mendeley Data assigns a provisional DOI to draft datasets. The issuing of a permanent DOI for Mendeley Data submitted datasets is carried out by the British Library via DataCite. It is used to make a document/reference uniquely identifiable from any other document/reference when your article is published and made available electronically. The DOI for a document remains fixed over the lifetime of the document.

Who owns and controls the data?

When you publish your data with our service, you choose a licence to publish it under, from a range of Creative Commons and open software licences. This means you retain control of the data, and choose the terms under which others may consume and reuse it. You may delete your dataset at any time, by contacting us.

Is my data stored safely?

Your data is stored on Amazon S3 servers, in Germany, where it benefits from redundancy and multiple backups. Our service has been extensively penetration tested and received certification. In addition, we partner with DANS (Data Archiving and Network Services - an industry-leading scientific data archive service), to preserve your data over the long-term. This means your dataset will be discoverable in perpetuity, via the DOI it is issued on publication. If you have any further questions, please contact us.

What is Mendeley Data's business model?

All services provided by Mendeley Data - storing, posting and accessing data - are free-to-use. In future, we may introduce a freemium model - for instance charging for storing and posting data, above a certain dataset size threshold. This will not affect existing datasets, which will continue to be stored for free. We will offer paid-for versions of our service to institutions.

Appendix G - data storage provision, backup services and data management plan by location.

Below are the initial results (Dec 2017) reproduced here as they give a good indication of provision across the partnership currently, and why there is a need for this framework. Displayed are the answers to four of 17 questions asked in a wider survey of data provision.

Academic Partner	Does your institution currently have a Research Data Management Policy?	The university is developing a partnership-wide RDM, Would you be interested in using such a resource?	At your Institution/Research Unit, where does the responsibility for Research Data Planning lie?	Is it part of the normal proposal process to create a DMP at your institution?
North Highland College	No - We have no policy in place or in development, Not that I know of	Yes	Principal Investigator	In some cases
North Highland College - ERI	No - We have no policy in place or in development, Not that I know of	Yes	Don't know/not sure	I don't think so
NAFC Marine Centre	No - We have no policy in place or in development, Not that I know of	Maybe	Individual Researchers	No - we rarely produce Research Data Plans
Centre for Health Sciences	No - We have no policy in place or in development	Yes, It needs to be simple and researcher-led	Principal Investigator	This is usually a standard part of an IRAS application for studies that require NHS ethical approval.
Executive Office	Not altogether sure	Maybe	Don't know/not sure	No - we rarely produce Research Data Plans
Lews Castle College	No - We have no policy in place or in development	Yes	Principal Investigator	No - we rarely produce Research Data Plans
Shetland College	No - We have no policy in place or in development	Yes, Simple things - Where should research data be stored? How long for? Etc.	Assume the responsibility rests with the PI of each project, but I don't know.	I don't know
NAFC Marine Centre	No - We have no policy in place or in development	Yes	Principal Investigator, Head of Research, Research Institution, Member of Senior Management Team with responsibility for Research	Don't know/not sure
SAMS	Yes - We are happy with our own policy	Maybe	Principal Investigator	Yes, in most cases
Moray College	No - We have no policy in place or in development	Maybe	Don't know/not sure	Don't know/not sure
Centre for Health Sciences	No - We have no policy in place or in development	Yes	Research Committee would oversee this	Research Committee would oversee this

Appendix H - GDPR key changes

Details taken from, and much more information/further reading at: ***EUGDPR.org***
Specific UHI GDPR toolkit available from the ***UHI website****.*

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below.

Increased Territorial Scope (extra-territorial applicability)

Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high profile court cases. GPDR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-Eu businesses processing the data of EU citizens will also have to appoint a representative in the EU.

Penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g.not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Consent

The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Data Portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At it’s core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - 'The controller shall implement appropriate technical and organisational measures in an effective way in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers

Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

1. **Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices**
2. **May be a staff member or an external service provider**
3. **Contact details must be provided to the relevant DPA**
4. **Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge**
5. **Must report directly to the highest level of management**
6. **Must not carry out any other tasks that could results in a conflict of interest.**

Appendix I - RDM Training Programme

RDM policy and guidelines dissemination – help and support

At a meeting 17th May 2018 to discuss the provision of help and training, as detailed in section 5 of the RDM policy, the following provision was agreed:

a) An annual set of RDM sessions appearing at no less than 5 locations will be organised; face to face sessions and Q&A sessions at partner locations for groups of researchers and students. The leaders at these events will be:
    1. The University Librarian
    2. The Research Information Systems Officer
    3. The Data Protection Officer
    4. A representative from LIS/local ICT teams

These events will aim to explain the RDM policy and guidelines, instil the principals of 'best practice' when dealing with research data and aim to answer any questions arising from the presentation.

b) Online guides to be developed to aide availability of access to the policy, guide and background information. This will take the form of a webpage within the existing 'Research Resources' area of the university website and a Libguide within the libraries area which will complement rather than duplicate each other. These will be published immediately the policy is approved at RKEC and updated as required.

c) Additional information will be added to the existing session that already covers elements of dealing with research data within the PhD Induction days (run in March and October). This will help to ensure that new PhD students will start off down the correct path.

d) Sessions and/or a conference table will be organised at every Research Conference, these currently occur on a biennial basis.

This will mean the university will provide annual sessions at partner locations, biannual sessions for all new PhD students, biennial reminder sessions for staff and students and perennial information on web and Libguide.

It was concluded that the best time to catch as many research staff and students as possible was at the beginning of the academic year, but just after the very busy initial weeks. Therefore, we will be making arrangements for the annual series of sessions during the third week of September.