University of the Highlands and Islands
Oilthigh na Gàidhealtachd agus nan Eilean

Research Data Management Policy

The University Partnership adopts the following policy on Research Data Management. It should be noted elements of the policy model are aspirational, and that full implementation may take some years.

1. Research data will be managed to the highest standards throughout the research data lifecycle as part of the University Partnership's commitment to research excellence.
2. Responsibility for establishing a sound research Data Management Plan (DMP) during any research project or programme lies primarily with Principal Investigators (PIs) but will be facilitated by processes at the local institution.
3. All new research proposals must include research data management plans or protocols that explicitly address data capture, management, integrity, confidentiality, retention, sharing and publication. Retention periods for all data should, as a minimum, conform to the requirements of a funding agency or body.
4. Research data management plans must ensure that research data and metadata is available for access and re-use where appropriate and under appropriate safeguards. Personal data of all subjects of research data must be protected. Additionally, use of others' data should always conform to legal, ethical and regulatory frameworks including the appropriate acknowledgement.
5. The University Partnership will provide training, support, advice and, where required, guidelines and templates for research data management and development of research data management plans.
6. The University Partnership will provide mechanisms and services for storage, backup, registration, deposit and retention of research data assets in support of current and future access, during and after completion of research projects. All data and metadata records added to the institutional repository will be curated in perpetuity by the University Partnership as it currently exists or however it may be constituted in the future.
7. A record of any research data produced across the University Partnership will be recorded within the university's Research Management System (currently PURE), with metadata records available to external viewers, where appropriate. Where data is not to be made publically available for a defined reason, this will be stated on the Research Management System (RMS).
8. Research data of future historical interest, and all research data that represent records of the University Partnership, including data that substantiates research findings, will be offered and assessed for deposit and retention in an appropriate national or international data service or domain repository, or the university RMS. Ensure compliance with point 9 of this policy.
9. Any data which is retained elsewhere, for example in an international data service, discipline specific repository or domain repository must be recorded on the RMS (see section 7).
10. Exclusive rights to reuse or publish research data should not be handed over to commercial publishers or agents without retaining the rights to make the data openly available for re-use, unless this is a condition of funding or a condition of a commercial or government contract.

University of the Highlands and Islands
Oilthigh na Gàidhealtachd agus nan Eilean

Research Data Management Guidelines

Table of Contents

Definition, Scope and Purpose of the RDMP & Guidelines

Definition

For the purposes of this document and the UHI Research Data Management Policy we use the definition for research data outlined in the publication '*Concordat on Open Research Data*' published July 2016 and written jointly by Universities UK, HEFCE, RCUK and Wellcome Trust:

"Research data are the evidence that underpins the answer to the research question, and can be used to validate findings regardless of its form (e.g. print, digital, or physical). These might be quantitative information or qualitative statements collected by researchers in the course of their work by experimentation, observation, modelling, interview or other methods, or information derived from existing evidence. Data may be raw or primary (e.g. direct from measurement or collection) or derived from primary data for subsequent analysis or interpretation (e.g. cleaned up or as an extract from a larger data set), or derived from existing sources where the rights may be held by others. Data may be defined as 'relational' or 'functional' components of research, thus signalling that their identification and value lies in whether and how researchers use them as evidence for claims.

They may include, for example, statistics, collections of digital images, sound recordings, transcripts of interviews, survey data and fieldwork observations with appropriate annotations, an interpretation, an artwork, archives, found objects, published texts or a manuscript. "

The separate document 'UHI RDM appendices' details all standards, concordat, regulatory requirements and definitions incorporated into this policy document.

Scope

Within the scope of this policy is all data generated as a result of research work while in the employment the university or the academic partners - funded or un-funded work, short-term or archival. Provision should be made for the storage of both working data and for long-term archival of research results and associated data.

Purpose

The policy is intended to form a UHI-wide framework on research data management and provide clear guidelines to research staff to follow when developing projects. This will ensure institutional research data is captured, stored and curated securely and in line with sector and discipline standards, and will meet various regulatory requirements, thereby mitigating the risk of loss or non-compliance. The numbered sections of the Guidance Document mirror and expand on the points outlined in the Research Data Management Policy. Together they are intended as non-exhaustive guidance to assist university research staff to comply with the university policy, requirements of funding bodies, government legislation and legal requirements.

The RDM policy and this guide document will be reviewed on an annual basis in April by representatives from the Research Office, University Libraries, Learning & Information Services, and updated where necessary for approval by the university Research and Knowledge Exchange Committee (RKEC).

Any questions on this policy should be directed to:
RO@uhi.ac.uk

Section 1 – Data lifecycle

Research data will be managed to the highest standards throughout the research data lifecycle as part of the University Partnership's commitment to research excellence.

Research data lifecycle can be described as: creation, curation, analysis, preservation, access and eventual disposal. In a wider sense this could involve the following steps:

1) Plan how to manage the data (e.g. creating a Data Management Plan or DMP).
2) Do the research and create/analyse/use data.
3) Decide what data to keep/make accessible, who for and why.
4) Thinking about and resolve issues around ethics, security, privacy and data protection.
5) Deposit into a discipline-specific repository or institutional repository.
6) Registration on DataCite and the UHI RMS (PURE).
7) Publish papers, reference the data, disseminate the findings, promote the data.

Section 2 – Data Management Plan (DMP) responsibility

Responsibility for establishing a sound research Data Management Plan (DMP) during any research project or programme lies primarily with Principal Investigators (PIs) but will be facilitated by processes at the local institution.

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 programme or project will be responsible for developing a project specific DMP, section 3 describes this in more detail.

Appropriate funding for RDM should be requested for every new funding application, where this is an eligible cost item allowed by the funder. Your local ICT team or data manager can help with indications of data storage costs. Where the research is unfunded the data still falls within scope of this policy.

Section 3 – Initial DMP considerations

All new research proposals must include research data management plans or protocols that explicitly address data capture, management, integrity, confidentiality, retention, sharing and publication. Retention periods for all data should, as a minimum, conform to the requirements of a funding agency or body.

Developing a Data Management Plan (DMP)

Data Management Plans should always be developed as part of writing any funding application; indeed many funders will require a DMP as part of an application. At the very least, an outline DMP should list all the expected data to be generated. This will allow the development of a full DMP which should account for the correct acquisition and analysis (e.g. through Data standards, SOPs), security (access & backup), anonymising (where applicable), accessibility, licencing, funder requirements, DOI creation, repository choice, curation and preservation of the research data into the future (likely to be beyond the life of a research project). When

creating a plan, your funder policy must take precedence. If any part of the funder policy is at odds with University Partnership policy you must raise this with the person responsible for research/records management at your institute or department to arrive at a resolution acceptable to all parties.

Should you have no specified local policy, **DMP Online** have an extensive section with guidance and templates dedicated to the development and management of data plans – it is backed by the Digital Curation Centre (DCC). This will take you through the steps of estimating the amount and type of storage you might require for the data you produce during your (prospective) project – this can be anything from 1Gb to many Tb – but it is important, no matter what the size of the data gathered, that you have plan for storage, management and curation.

Quantify and cost your data storage needs

The requirement to identify and quantify your expected storage needs will allow you to build the cost of the storage into your funding application. The university Grants and Contracts Office (GCO) will ask for this information as part of every funding application. For help with estimating storage costs see section 6. Be aware that the overall storage period may be longer than the research project so you need to be aware of the long term cost of this and build it into the funding application.

Retention Periods

You should always first refer to the requirements laid down by the funders of the research you are undertaking. The university Grants and Contracts Office (GCO) can help you discover this as it will always be stated in the terms of any funding arrangement. Please make yourself aware of any retention requirements, particularly where data contains information covered under GDPR (specifically personal data), see section 4. Some funders, may specifically require any data be ingested at funder based Data Access centres (e.g. RCUK), all other science data should be curated according to discipline norms.

Section 4 – Availability and re-use of data

Research data management plans must ensure that research data and metadata is available for access and re-use where appropriate and under appropriate safeguards. Personal data of all subjects of research data must be protected. Additionally, use of others' data should always conform to legal, ethical and regulatory frameworks including the appropriate acknowledgement.

Considerations within your Data Management Plan (DMP)

When constructing DMP's you must:

1. Respect the principles of the **university ethics policy** and **NHS ethics policy** (where dealing with any NHS patients or patient data).
2. Plan to store any personal data within the terms of the **UK Data Protection legislation** and comply with the legal framework known as General Data Protection Regulation (GDPR). The UK is implementing this framework despite exiting the EU. GDPR policy is outwith the scope of this document: further guidance is available on the **governance webpages**, here you should pay particular attention to complying with the points laid out in the Privacy Impact Assessment (PIA), the template and guidelines for which are available on **SharePoint**. All new projects must complete a PIA as part of agreeing a DMP.
3. Ensure the correct visibility of the data.
4. Include a data use statement.
5. Ensure it is approved by the appropriate person at your location.

Ethics Policy

Ethics policy and ethical issues raised by your research proposal must be considered when developing your research project. The ethics team have **web resources** giving guidance and resources for developing your research proposal, planning your research project ethically and submitting an application for ethical approval. The university **Research Ethics Framework document** gives full details of this process.

Additional to the university ethics policy, if you are dealing with any NHS patient or patient data you must also follow the guidelines laid out by NHS Highland and access their **NHS ethics toolkit** .

Safeguarding personal data

GDPR policy is outwith the scope of this document but it is nonetheless crucial to understand it's implications as they relate to data storage and use of personal data that may be held: further guidance is available on the university **governance webpages**.

Data protection and Freedom of Information

Anything added to a database is subject to the Data Protection legislation, Freedom of Information (Scotland) Act 2002 (FOISA) and Environmental Information Regulations (EIR). You should always ensure you only add data that is correct, pertinent to the subject and that does not infringe any of the safeguards contained in the Data Protection Legislation. Additionally, any data held on a UK database could be subject to a 'Freedom of Information Request', or FOI, where anyone can request to see the information we hold on them, or on a particular subject. In line with university policy on FOI please refer all requests immediately to **foi@uhi.ac.uk** .

NOTE: (1) FOI does not always apply to SAMS as data related to SAMS can be exempt from FOI obligations. If you are unsure check with the SAMS FOI officer. (2) NAFC is also exempt from FOI obligations; this is due to having Charitable Trust status. (3) EIR may or may not apply at SAMS – if you are unsure check with SAMS head of ICT.

While working with any data, it must be remembered at all times that each piece of information has its own sensitivity. There may be a requirement to make an output publically available as part of the agreement to fund the research but there could be commercial sensitivity surrounding the project in total. The level of access, version made public and any embargo dates must be assessed for sensitivity (e.g. national defence, commercial etc) and any requirements included in your DMP.

Contact the university Data Protection Officer at **dataprotectionofficer@uhi.ac.uk** if you need specific questions clarified.

Visibility of Your Data

Any entry added to the institutional RMS (currently PURE) as well as any discipline specific repository must include the appropriate visibility setting (taking into account subject, funder, commercial, REF and departmental needs). This setting indicates to the RMS if the public portal (**the UHI Research Database**) is allowed to display details of the data, and therefore if the data is available to anyone with an internet connection or if the data is confidential. For example, most funders now require any data produced from research they have funded be made openly available to anyone with an internet connection. But certain commercial work may have to be kept confidential – this should be set appropriately within the RMS, with the default position being to make all data openly available. The person adding data has responsibility to ensure the correct level of visibility is set on each piece of data.

Re-use of other researchers data

All research data should have a data use statement included, which must always be adhered to.

Approval of Data Management Plans

Once you have your plan completed, this must be signed off by your local Head of Research or Head of ICT (depending on local arrangements) before your funding application is submitted.

Section 5 – Help and support

The University Partnership will provide training, support, advice and, where required, guidelines and templates for research data management and development of research data management plans.

The university advocates the use of existing online resources available through **DMP Online**. This extensive selection of guidance and templates dedicated to the development and management of data plans is backed by the Digital Curation Centre (DCC). Specific disciplines may have their own requirements – such as the marine science field where MEDIN provides training, data standards and data discovery services – always refer to your local Head of Research or Head of ICT if you are unsure. More information on MEDIN is available in Appendix E of this document and on the **MEDIN** website.

The university will provide annual refresher sessions for staff and students at partner locations (September), biannual sessions for all new PhD students (March and October induction), biennial reminder sessions at the Research Conference and perennial information on the university webpages and Libguides, where assistance via email will be available. These will be advertised locally in libraries and in university newsletters.

Section 6 – Institutional storage services

The University Partnership will provide mechanisms and services for storage, backup, registration, deposit and retention of research data assets in support of current and future access, during and after completion of research projects. All data and metadata records added to the institutional repository will be curated in perpetuity by the University Partnership as it currently exists or however it may be constituted in the future.

All research data should be stored and accessed only on approved systems agreed in advance with your local ICT or data management team. Specific requirements for specialist servers (e.g. linux) for processing , storing or delivering data (e.g. GIS, webservices like GeoServer or ERDDAP) or requirements for expertise in designing, managing and visualising data should all be discussed with your local ICT or data management team and the outcomes built into your DMP.

The ICT teams of the University Partnership will be responsible for managing the systems and equipment used to store data. Approved systems includes the devices and services managed by the University Partnership for the purposes of research data management but can also include, after due diligence, data collected and stored on collaborators' systems. If using external services, you must be aware of the security and backup facilities provided and ensure they comply with your funder and University Partnership requirements. You should also be clear where the data servers are located as GDPR legislation requires that all personal data is stored within the EU. GDPR policy is out-with the scope of this document but it is nonetheless crucial to understand its implications as they relate to data storage: further guidance is available on the university **governance webpages.**

Should data be required to be stored externally of Academic Partner systems please pay special attention to section 9 of this policy.

Any system or device used that is not approved runs the real risk of research data being lost, inappropriately shared or being insecure to external threat.

All staff, contractors, consultants, interns and suppliers are bound by the terms of this policy. For collaborations where data may be collected and\or stored on collaborators' systems it is the responsibility of the university researcher to ensure the systems and policies employed by the collaborator have similar safeguards in place as outlined in this policy.

Avoiding data loss

Use of approved systems also ensures University Partnership data can have the appropriate visibility and access settings (according to the requirements surrounding any piece of data) and that all data is backed-up to protect against data loss. The University Partnership has implemented specific systems and carefully managed controls to protect all data stored on authorized systems. Shared drives and SharePoint (or specific project servers/drives) are backed-up according to our data storage policies and are secured with appropriate firewalls.

Data created during the term of any short-lived project should be deposited as soon as possible but always before the end of any project. All data generated, from any project, must be deposited on institutional network storage, as soon as possible, where it will be securely backed up and preserved in its original state.

It should also be remembered that data must be deposited on institutional network storage should a member of research staff or student decide to leave the university – all PI's and HR departments have responsibility to ensure the capture of any research data well in advance of any staff members leaving the university.

Data should initially be stored with sufficient provenance documentation to make it identifiable and re-useable in future.

Security and Access

It is important that you keep your research data safe and secure while you are working on them. Data security involves ensuring that only authorised people have access to read, edit or use your data. This protects against both inappropriate disclosure of information and malicious or accidental modification.

Short-term data storage

All data generated, from any project, must be deposited on institutional network storage, as soon as possible, where it can be securely backed up and preserved in its original state. This is to ensure that all University Partnership data, files and client, supplier, and other business information is properly secured and protected from accidental loss or unauthorized use.

In the first instance researchers should contact their local ICT or data management team to discuss their particular technical and data storage needs. If in doubt please contact the UHI Servicedesk who will direct you to the right person.

Archiving and long-term data storage

Long-term curation of research data secures its ongoing accuracy, authenticity, reliability and readability. It is also ensures specific funders and/or sponsor's requirements are met.

Discipline specific repositories can be used where they exist as they will have expertise in handling the data from that field.

The university is currently investigating an appropriate service for the long-term data storage of research data. Please refer to your local ICT team or data manager for interim arrangements and for help with indications of storage costs.

Discipline specific repositories can be used where they exist as;

1. They are experienced in handling data from that field

2. It's where others (researchers, industry) go to source data

3. They offer DOI registration too

Commercial service for long-term data storage

The university has an arrangement with an external, commercial long term data storage company for the archiving of data that is no longer considered working sets.

Any such arrangement will be agreed on the basis that the company can pledge a guarantee of data integrity for the lifetime of the data and have experience of handling data from industry, health, financial services as well as Higher Education research. Services such as these are dedicated to ensuring data is accessible and update any redundant file types to be available on current software programs. The service will be procured through an existing framework agreement with JISC, ensuring no additional tendering process is required.

To access this service, please apply through the Servicedesk: helpdeskmail@uhi.ac.uk .

Mendeley Data Service for long-term dataset storage

One option for long term preservation of your research data could be a data service from Mendeley. Mendeley have teamed up with DANS (Data Archiving and Networking Services) to create a long term preservation service with DOI minting capability. All published datasets will be sent offsite to DANS, where they will ensure that your data is safely archived. Your published research data will include a Force11 compliant citation so that other researchers can cite your research along with provision of a unique DOI for each version of your dataset ensures your dataset's citation will always be valid.

Should you use this service you must ensure you comply with **section 9** of this policy. There is more detail on this service in Appendix F

Further information, registration and uploads at **https://data.mendeley.com/**

Curation of digital data

This subject is beyond the scope of this policy but the concepts should be considered in the development of a DMP. A summary of the concepts is outlined below but you should refer to the web pages of the **Data Curation Centre** for more detailed information.

What is meant by digital curation?
Digital curation involves maintaining, preserving and adding value to digital research data throughout its lifecycle. The active management of research data reduces threats to their long-term research value and mitigates the risk of digital obsolescence. Meanwhile, curated data in trusted digital repositories may be shared among the wider UK research community. Curation enhances the long-term value of existing data by making it available for further high quality research.

Planning the ongoing process
Because digital curation and data preservation are ongoing processes, you must plan for preservation throughout the lifecycle of digital material. Preservation actions must be planned – and then realised – to ensure that the authoritative nature of digital material is protected for the long term. Such actions include validation, assigning preservation metadata, assigning representation information and ensuring acceptable data structures or file formats.

The digital curation lifecycle

Digital curation and data preservation are ongoing processes, requiring considerable thought and the investment of adequate time and resources. You must be aware of, and undertake, actions to promote curation and preservation throughout the data lifecycle from concept to re-use.

Section 7 – Recording institutional data

A record of any research data produced across the University Partnership will be recorded within the university's Research Management System (currently PURE), with metadata records available to external viewers, where appropriate. Where data is not to be made publically available for a defined reason, this will be stated on the Research Management System (RMS).

An entry must be added to RMS as well as any discipline specific repository with the appropriate visibility set (taking into account funder, commercial, REF or departmental needs) including links to the repository where the data is available. If the work is confidential, mark the visibility in the RMS as such, add a bibliographic note detailing why it is confidential and for how long to ensure the data can be accurately curated into the future. Visibility considerations are discussed in section 4 above.

For all externally held data an entry must be added to PURE to act as our registry of externally held data. The metadata entry in PURE should include a clear description of what the database is, how and where it was produced and links to the data source and any supporting files (usually on discipline specific databases or storage providers).

All university research data should have a data use statement included as a bibliographic note, or have the re-use licence stated as part of the DOI or full text record on the RMS.

Section 8 – Historical data

Research data of future historical interest, and all research data that represent records of the University Partnership, including data that substantiates research findings, will be offered and assessed for deposit and retention in an appropriate national or international data service or domain repository, or the university RMS. Make particular reference to section 9 of this policy.

Compliance with all other section guidance is assumed.

Section 9 – Data retained externally

Any data which is retained elsewhere, for example in an international data service, discipline specific repository or domain repository must be recorded on the RMS (see section 7).

External data repositories

Should it be decided (or required by a funder or a discipline standard) that the most appropriate storage is on an external repository or data store it is the responsibility of the PI leading a research project to ensure any

external storage solution complies with all the same policies and provisions laid out within this document. Security, visibility, access and funder requirements must all be assessed.

In these cases, the metadata entry in PURE should include a clear description of what the database is, how and where it was produced and links to the data source and any supporting files (usually on discipline specific databases or storage providers), in compliance with section 7 of this policy.

Marine Sciences data

MEDIN standards are the standard for Marine Sciences datasets and require deposits to be described by up to 30 metadata elements, whereas PURE has 19 elements. A PURE entry cannot currently comply to MEDIN metadata standards but it was not developed to do so as entries within PURE can come from any research discipline. This means that external arrangements must be made for depositing Marine Science datasets, while still complying with all other sections of this policy document. More information on the MEDIN standard and a link to the MEDIN webpage at Appendix E.

Section 10 – Rights and licencing

Exclusive rights to reuse or publish research data should not be handed over to commercial publishers or agents without retaining the rights to make the data openly available for re-use, unless this is a condition of funding or a condition of a commercial contract.

Publishing agreements are negotiated with your journal contact, and remember it is a negotiation – if you don't initially get what you want, request different terms. Generally it is in both your interests to get an article published so there is usually some space for agreeing a mutually beneficial arrangement, whether it be a more open licence, a shorter embargo or a discount on any Article Processing Charge (APC). If you are not the lead/corresponding author on an article then you should ensure the lead/corresponding author communicates the terms of any agreement to all authors. This can be tricky when the lead author is outside the UK, and therefore not subject to the same publishing and Open Access requirements that are required in the UK, but as a UK researcher it is your responsibility to ensure any article you are involved in meets the current UK requirements. Never agree to a contract that leaves you with no rights to your work.

Commercial/military sensitivity and copyright

If a dataset, or article with accompanying data, was funded by a commercial contract and a stipulation of gaining the contract and/or funding states that the results must be kept confidential then clearly you must respect this. Here, a metadata entry for the work should be added to the RMS (PURE), add a bibliographic note to the record detailing why the work is confidential, for how long and set the record as 'Confidential' in compliance with section 7 of this policy; this ensures you can see the record but no-one else can. If a commercial customer stipulates that you remove all the data at the end of contract- then clearly you must respect this, the metadata record on PURE should be annotated with a note declaring this and the record set as 'Confidential'.

Where a piece of work has been contracted by the government or the military, it is understood the terms of that agreement and national security issues could over-ride elements of this policy.

Copyright is beyond the scope of this guide, but for a useful description to use as a starting point, see Elsevier at **https://www.elsevier.com/about/company-information/policies/copyright**. Remember; other publishers may have differing rules and even some Elsevier-owned journals may have, the link is offered as a good baseline explanation of how research publishing within the Open Access environment affects what you can

and can't do with your outputs. You should always refer to your own publisher and funder for specific rules governing a specific article to work out the archiving and licencing conditions required.

UHI Intellectual Property Framework Guidelines, July 2012.

Licencing of research data or articles

Creative Commons licencing is the basis for most re-use agreements at the time of writing (2018) with a number of licencing regimes possible to ensure you get the best mix of sharing your work and retention of credit for the work.

University of the Highlands and Islands
Oilthigh na Gàidhealtachd agus nan Eilean

Data Management Checklist

Use this checklist to guide you through the elements of data management to consider as you develop a research Data management Plan (DMP) for your research project. This document is intended as a starting point to help you structure your planning process, not all information will be relevant to your project, and it should be used alongside the university research data management policy and guide at: Research policies.

Data Types

A description of the data your project will capture, create or use. It is important to record this detail to help you and subsequent users understand why and how the data were created.

» How will data be created (captured)?
e.g. interview data, questionnaires, imaging, experimental measurements etc.

» What data formats will be used?
e.g. file formats such as excel, word, open source etc. Consider choice of data formats such as: will the data formats meet certain specifications including international or national standards, widely used, is it accepted as best practice in this discipline, will it facilitate re-use?

» Will the data be reproducible?
What would happen if it got lost or became unusable later?

» How much data will there be and what will its growth rate be?
How often will it change?

» Will existing data be used? If so, from where, and what is the relationship to the existing data?

» Are there special tools or software needed to create / process / visualise the data?

Data Organisation, Documentation and Metadata

Organising, documenting and describing data is important in order to assure quality control and reproducibility of data.

» What metadata standards will be used?

» How will metadata be captured, created and managed? Is there a discipline-specific standard?

» How will folders and files be structured and named?

» How will different file versions be managed?

» What data identifiers will be assigned?

» What other documentation and contextual information will be available in order to help others understand the data?
e.g. data dictionaries, codebooks, questionnaires

Data Storage and Security

Storage

» Where and what media?
Short-term, longer-term

» Who will be responsible?

Back-up

» How will it be done and how often will it be done?

» Who will be responsible?

Security

» How will data security be guaranteed
e.g. data encryption, password etc.

» How will the data be shared during the project?

Long-Term Preservation

» What data will be kept or destroyed after the end of the project?

» How long will data be kept?
e.g. 3-5 years, 10-20 years, permanently?

» Where will the data be stored?
e.g. archive, data repository, network.

» What file formats will be used?
Are they long-lived?

» Who will manage the long term data?

- What is needed to prepare the data for preservation or data sharing?
- What related information will be deposited with the data?

Ethics & Intellectual Property

- Are there any ethical and privacy issues that may prohibit sharing of some or all of the data? If so, how will these be resolved?
- Do your data contain confidential or sensitive information?
  If so have you discussed data sharing with the respondents from whom you collected the data?
- Who owns the data arising from your research, and the intellectual property rights relating to them?

Data Sharing and Re-Use

- In addition to the owners of the data you generate, who else has a right to see or use this data? And who else should reasonably have access? Who will be the audience for your data?
- Are there any limits to data sharing required
- Are there any sharing requirements?
  e.g. funder data sharing policy
- How will the data be discovered and shared?
- What tools / software will be needed to work with the data?
- Will there be embargo periods?

Implementing Your Plan

- Who will be responsible for ensuring your plan is followed?
- How often will your plan be reviewed and updated?

Further information

Managing your Data

Increasingly funding organisations require that research data management is addressed in grant applications. Please refer to your local Head of Research for advice and to the guidelines outlined at:

Data Management webpage

Data Storage, Backup and Security

Refer to your local Research IT support team to discuss the options available to you regarding data storage or any of your IT requirements. If you have no local team contact the university IT support at:

servicedesk@uhi.ac.uk

Intellectual Property/Commercialisation

For queries regarding intellectual property and support for researchers interested in commercialization contact Joe Irvine, Head of Knowledge Exchange:

Joe.irvine@uhi.ac.uk

Further reading:

IP webpage

Research Ethics

The Research Ethics team can help with advice and consultations to establish any ethics considerations surrounding your project. Full details available on the Research Ethics webpage.

Further information from:
fiona.leiper@uhi.ac.uk