UK Research
and Innovation

# UKRI Information Management Policy

## Table of Contents

Policy Statement ....................1

Management Statement ....................2

References ....................2

1. Purpose and scope ....................3

2. Definitions ....................3

3. Relationship with existing strategies and policies ....................4

4. How we will create, organise, and store information ....................4

5. How we will use, access and share information ....................4

6. How and when we will dispose of information ....................5

7. Responsibilities ....................5

8. Approval and Review ....................6

9. Reporting and Management Requirements ....................6

10. Storage ....................6

## Policy Statement

UK Research and Innovation (UKRI) recognises that the effective management of information is necessary to:

- Support core business functions and decision making
- Comply with legal and regulatory obligations
- Contribute to the effective overall management of the organisation.

Information management applies to the creation of reliable, authentic and accessible information and the controlled management, retention and disposal thereof.

UKRI has identified information management as an essential corporate function and aims to ensure the necessary levels of organisational support to enable its effectiveness and public accountability.

## Management Statement

The Information Management Policy has been agreed with the Trade Union Side (JNCC) and by the Data and Information Governance Committee. The policy is managed by the Information Governance Group.

| Version Number | Status | Revision Date | Summary of Changes |
|---|---|---|---|
| Version 2.1 | Draft | September 2021 | Nicole Convery – Major revision of the UKRI Records Management Policy |
| Version 2.2 | Draft | October 2021 | Changes following review by IG group |
| Version 2.2. | Draft | November 2021 | Approved by DIGC without changes |
| Version 3.0 | Final | December 2021 | Final version following JNCC approval 17th December 2022 |

## References

1. Public Records Act 1958
2. UK General Data Protection Regulation 2016/679
3. Data Protection Act 2018
4. Freedom of Information Act 2000
5. Environmental Information Regulations 2004
6. Protection of Freedoms Act 2012
7. Lord Chancellor’s Code of Practice on the Management of Records under section 46 of the Freedom of Information Act 2000, July 2021

## 1. Purpose and scope

1.1. This policy provides a framework for managing UKRI information. It sets out best practice for the creation, use and disposal of information, regardless of format. The policy enables employees to:

1.1.1. create and capture accurate, authentic and reliable information
1.1.2. make informed policy and business decisions
1.1.3. feel empowered and confident working with information
1.1.4. be accountable and transparent
1.1.5. dispose of information that is no longer required
1.1.6. identify and protect vital information
1.1.7. comply with legislation and best practice
1.1.8. collaborate securely internally and externally, where appropriate
1.1.9. capture and preserve corporate memory
1.1.10. increase efficiency for staff and systems

1.2. UKRI is a public record body covered by the Public Records Acts of 1958 and 1967 and is required by law to manage its records in accordance with its legal and regulatory environment. UKRI adheres to the Lord Chancellor's Code of Practice on Records Management and other relevant records and information management related standards and regulations.

1.3. This Policy applies to the management of UKRI information in the corporate hub, research councils, Research England and Innovate UK. It applies to corporate information held in UKRI centres, units and institutes but not to scientific or primary research information and related materials.

1.4. The management of UKRI data is defined in the Data Strategy owned by the Strategy group. The Knowledge and Information Management (KIM) team will work with the Strategy group to support the management of data in accordance with the strategy.

1.5. This policy applies to all UKRI employees, workers, contractors and visitors.

## 2. Definitions

2.1. *Information* at UKRI consists of data (or structured information), records and documents (unstructured information).

2.2. *Data* [will be defined in the Data Strategy and the definition will be added when available].

2.3. *Records* are defined as all information which provides evidence of business activity and for which there are legal, regulatory and business requirements for retention. Records are subject to destruction rules but may have permanent historic value.

2.4. *Documents* are defined as information which has immediate or operational value but that does not have corporate value/provide evidence of business activity. Documents should not be kept for longer than necessary and usually no longer than 3 years.

2.5. An *Information Asset* (IA) can contain a number of records, documents and data. It is a body of information that is created and/or maintained by UKRI as a single unit, so it can be understood, shared, protected and exploited effectively. IAs have an identifiable and manageable value, risk, content and lifecycle.

2.6. More information management related terms are defined in the Glossary of Information Governance Terms.

## 3. Relationship with existing strategies and policies

3.1. This policy has been created within the context of existing UKRI strategies and policies:

3.1.1. KIM Strategy and delivery Plan 2020-2022
3.1.2. Information Governance Strategy 2019-2021
3.1.3. UKRI Retention Schedule
3.1.4. Data Protection Policy
3.1.5. UKRI Freedom of Information & Environmental Information Regulations Policy
3.1.6. UKRI Security Policy Framework
3.1.7. Government recordkeeping policy & GKIM Digital Record Keeping Strategy

## 4. How we will create, organise, and store information

4.1. All UKRI information must be stored in an appropriate, approved corporate information management system (i.e. SharePoint, Teams, Objective). Within the information management system records must be registered and version controlled to ensure authenticity and reliability.

4.2. UKRI is committed to creating and maintaining relevant and accurate records in both electronic and paper format of business activities. Appropriate information and processes must be in place to document decisions and activities. The retention schedule provides a framework for the identification of records that need to be kept as evidence of business activity (for more information see section 6.1)

4.3. All UKRI information must have sufficient metadata to be identifiable and accessible, and to provide administrative context needed for the effective management of the information.

4.4. All UKRI information assets are captured and described in the Information Asset Register (IAR) and managed by the information asset owners.

## 5. How we will use, access and share information

5.1. All UKRI information should be open to staff as required as part of their role. Information which is sensitive or protected will be closed by exception.

5.2. UKRI is committed to support a collaborative, hybrid working environment and information can be shared securely in accordance with its sensitivity and in line with the UKRI Data Protection and Security Classification Policies and associated handling guidance. Staff should make use of authorised corporate collaboration tools only.

5.3. In certain circumstances UKRI is obliged to prevent the scheduled destruction of information and apply a temporary preservation hold to information that might pertain to the following cases (the list is not complete):

5.3.1. Information rights requests
5.3.2. Complaints and whistleblowing
5.3.3. Legal, HR, Fraud and Research Integrity cases
5.3.4. Public Inquiries under the Inquiries Act 2005 and The Inquiry Rules 2006
5.3.5. Investigations by Regulators such as the Information Commissioners' Office

5.4. The preservation hold process is owned by the SIRO, managed by the KIM team and technically executed by DDaT.

## 6. How and when we will dispose of information

6.1. Information must only be retained for as long as it is needed to meet UKRI's business need and relevant legal and regulatory requirements. The UKRI retention schedule specifies for each of UKRI's functions the period of time for which each class of records needs to be retained to fulfil these requirements. Documents should be destroyed no later than 3 years after creation when their operational value has ceased.

6.2. The UKRI retention schedule applies to all UKRI records and is applied to records created by councils prior to UKRI's formation in April 2018. Councils can apply for an exemption from this rule, should there be compliance or significant business reasons preventing the implementation of the schedule to legacy (pre-2018) records.

6.3. Information retention will be managed 'in place' in UKRI's portfolio of corporately approved information systems in line with government strategy. All UKRI information systems must have relevant retention functionality or approved processes for the management of retention.

6.4. The destruction of information past their retention date will be executed automatically (i.e., without asset owner review) to reduce the burden on asset owners and improve efficiency. We perceive this as an aspiration in line with best practice and government expectations to be progressed where technology and risk appetite allow.

6.5. Records which demonstrate the significance of the functions and activities of UKRI and which provide information relevant to the public are transferred to The National Archives (TNA) for permanent preservation in time to meet the requirements of the 20-year rule. The selection and transfer of corporate records is handled in line with TNA's Appraisal Policy and its general guidelines for the selection of records.

6.6. Records that have been selected for permanent preservation at TNA are reviewed, prior to transfer, for sensitivity in regard to UKRI's obligations under the UK General Data Protection Regulations (GDPR) and Data Protection Act 2018.

## 7. Responsibilities

7.1. All members of staff are responsible for the proper management of the information they create and use in accordance with the UKRI Information Management Policy and guidance relating to information management.

7.2. Information Asset Owners are responsible for

7.2.1. approving information assets on the Information Asset Register,
7.2.2. controlling access to the assets they own,
7.2.3. owning any associated information risks and mitigating actions,

7.2.4. completing an annual assurance process to ensure information is up to date,

7.2.5. authorising the disposal of information that has reached the end of its retention period.

7.3. The Knowledge and Information Management Team are responsible for

7.3.1. implementing and monitoring the policy and information management guidance,

7.3.2. the developing and implementing the retention schedule,

7.3.3. providing advice, guidance and training to all UKRI staff.

7.4. The Knowledge and Information Management (KIM) team is authorised to and will manage all UKRI information on behalf of information asset owners (IAO), including the business management of relevant information systems, the administration of disposal action and appraisal of information for permanent preservation.

7.5. The Departmental Records officer (DRO) is responsible for

7.5.1. monitoring and auditing UKRI's compliance with information management legislation and standards

7.5.2. advising UKRI on all aspects of information management legislation and standards

7.5.3. acting as a point of contact for the National Archives and the Lord Chancellor regarding compliance with the Public Records Act.

7.6. Directors are responsible for

7.6.1. making all employees within their Directorate aware of this policy as necessary,

7.6.2. ensuring that appropriate processes are implemented for managing information in line with this policy and information management good practice

## 8. Approval and Review

8.1. This policy should be regularly reviewed and agreed upon by management and Trade Unions, to incorporate any legislative change.

## 9. Reporting and Management Requirements

9.1. Compliance with this policy is measured and reported in several ways across UKRI

9.1.1. KIM capabilities and outputs are measured through the KIM Balanced Scorecard.

9.1.2. KIM maturity is measured annually through the Annual BEIS KIM Maturity Model and Self-Assessment Report.

9.1.3. Compliance with information legislation such as the Public Records Act is monitored through the Integrated Governance Risk and Assurance Framework (IGRAF).

9.1.4. Progress against the IG strategy and the KIM delivery/work plan is monitored by the Data and Information Governance Committee through quarterly updates.

## 10. Storage

10.1 This policy will be made available on the UKRI Website, employee intranets and via the policy register.