UK Research and Innovation

Data Protection Policy

Table of Contents

Policy Statement

UK Research and Innovation (UKRI) understands the importance of protecting personal information and is committed to complying with the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR). UKRI aims to foster a culture of transparency and accountability by demonstrating compliance with the principles set out in the legislation.

The DPA 2018 and the UK GDPR together set out the rules for how organisations must process personal data and sensitive, or special category, data about living individuals. It gives individuals a number of rights including, the right to find out what personal data is held about them by organisations and to request to see, correct or erase personal data held.

UKRI needs to collect and process personal data about people, including employees and individuals with whom it interacts with. This is done lawfully and appropriately by handling personal data in order to:

- Operate its daily business.
- Exercise its responsibilities and duties of care as an employer.
- Fulfil its statutory functions and duties.

UKRI is committed to ensuring that employees are appropriately trained and supported to achieve compliance with Data Protection legislation.

Management Statement

This policy is approved by the People, Finance and Operations Committee and subject to JNCC consultation. The policy is managed by the Information Governance Group.

Version Number	Status	Revision Date	Summary of Changes
Version 1.0	Published	01/03/19	New policy created
Version 1.1	Draft	28/01/21	Updated references to UK legislation, clarified definitions and expanded sections outlining data subject rights, UKRI responsibilities and data breach incidents.
Version 1.2	Draft	09/02/21	Incorporated comments from the Data and Information Governance Committee (DIGC)
Version 1.3	Draft	29/03/21	Incorporated comments from HR Policy Working Group and PFO discussion.
Version 2.0	Final	27/05/21	Cleared by JNCC and PFO, published as amended above.
Version 2.1	Final	18/08/21	Clarified definition of Personal Data and added references to UK GDPR Articles.
Version 2.2	Final	27/09/21	Updated Contents table, minor grammar corrections.
Next revision due		31/03/23	

1. Purpose

1.1 This policy applies to all personal data and special category personal data collected and processed by UKRI in the conduct of its business and applies to both automated personal data and to manual filing systems. Additional information to supplement the policy will be provided in the Appropriate Policy Document relating to special category and criminal offence data.

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

2. Definitions

2.1 Personal data as defined in the UK GDPR;

2.2 **Personal data:** 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[1]

2.3 **Special categories of personal data:** personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data (used for identification purposes), health data, or data concerning a person's sex life or sexual orientation[2].

3. Data protection principles

3.1 To ensure compliance with data protection legislation UKRI must ensure that personal data is handled in line with the following principles:

3.2 **Lawfulness, fairness and transparency**. In practice this means:

3.2.1 having a legitimate ground for collecting and using personal data,

3.2.2 not using personal data in a way that would have an adverse effect on the individual concerned,

3.2.3 being transparent about how you intend to use personal data and provide privacy notices where appropriate,

3.2.4 handling personal data in a way that the individual would reasonably expect,

3.2.5 ensuring that you do nothing unlawful with personal data,

3.2.6 special category data is only processed in line with the specified conditions set out in the relevant legislation.

[1] Article 4(1) UKGDPR: https://www.legislation.gov.uk/eur/2016/679/article/4
[2] Article 9(1) UKGDPR: https://www.legislation.gov.uk/eur/2016/679/article/9

3.3 **Purpose limitation.** Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In practice this means:

3.3.1 being clear about why you are collecting personal data and what you will do with it,

3.3.2 providing privacy notices and transparency information to ensure the purpose is communicated clearly,

3.3.3 ensuring that any additional processing of personal data is fair.

3.4 **Data minimisation**. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. In practice this means:

3.4.1 only processing the personal data that is necessary.

3.5 **Accuracy.** Accurate and, where necessary, kept up to date. In practice this means:

3.5.1 taking reasonable steps to ensure the accuracy of any personal data held,

3.5.2 ensuring that the source of the personal data is clear,

3.5.3 carefully considering any challenges to the accuracy of personal data

3.5.4 considering whether it is necessary to update the information.

3.6 **Storage Limitation**. Not kept for longer than is necessary for the purpose. In practice this means:

3.6.1 reviewing the length of time you keep personal data for, taking account of UKRI's retention schedule,

3.6.2 securely deleting information that is no longer needed.

3.7 **Integrity and confidentiality.** Processed in a manner that ensures the security of data using appropriate technical and organisational measures against unauthorised or unlawful processing, loss, damage or destruction. In practice this means:

3.7.1 designing and organising security to fit the nature of the personal data held and the harm that may result from the breach,

3.7.2 ensuring that the right physical and security measures are in place, backed by robust policies and procedures and reliable, appropriately trained employees,

3.7.3 reporting security breaches promptly so that they can be reported to the Information Commissioner's Office (ICO) within the required 72 hours timescale.

3.8 In addition, the first principle requires that one or more grounds for processing must be satisfied for the processing to take place. Many of these relate to the purpose for which you intend to use the data and the nature of the personal information.

3.9 UKRI, as the Data Controller, is responsible for and must be able to demonstrate compliance with these principles.

3.10 Further information on requirements relating to the processing special category data and data relating to criminal convictions, offences or related security measures will be set out in the Appropriate Policy Document.

4. Responsibilities

4.1 All employees are responsible for ensuring that they meet the requirements of UK data protection legislation and should familiarise themselves with this policy and related documents.

4.2 **UKRI has a responsibility as a Data Controller (or when acting as a joint Data Controller or a Data Processor) for:**

4.2.1 complying with Data Protection law and holding appropriate records,

4.2.2 ensuring appropriate agreements are in place with joint Data Controllers and Data Processors and that they are made aware of this policy as relevant,

4.2.3 cooperating with the Information Commissioner's Office, as the UK regulator of data protection law, and,

4.2.4 responding to regulatory/court action and paying administrative levies and fines issued by the Information Commissioner.

4.3 **The Data Protection Officer is responsible for:**

4.3.1 monitoring and auditing UKRI's compliance with data protection law, including the overall risk profile, and reporting annually to senior management boards,

4.3.2 advising UKRI on all aspects of its compliance with data protection law (including overseeing use of data protection impact assessments (DPIAs),

4.3.3 acting as UKRI's standard point of contact with the Information Commissioner's Office regarding data protection law, including in the case of personal data breaches; and,

4.3.4 acting as an available point of contact for complaints from data subjects.

4.4 **The Information Governance Group, in collaboration with other relevant teams working to support data protection compliance across UKRI, are responsible for:**

4.4.1 providing advice, guidance, training and tools/methods, in accordance with UKRI's overall risk profile and having considered the advice of the Data Protection Officer, relevant case law and ICO/other regulatory guidance, to help employees comply with this policy,

4.4.2 publishing and maintaining core privacy notices and other UKRI data protection documents,

4.4.3 handling data subject rights requests; and,

4.4.4 as advised by the Data Protection Officer, managing and/or handling data protection impact assessments, data subject complaints and personal data breaches.

4.5 **Directors are responsible for:**

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

4.5.2 ensuring that employees will have access to personal data only where it is required as part of their role,

4.5.3 ensuring that appropriate processes are implemented to enable information assets containing personal data within their directorate to be managed appropriately to enable compliance with data protection law; and.

4.5.4 ensuring the Data Protection Officer is involved, in a timely manner, on all issues relating to the protection of personal data, that the Data Protection Officer is sufficiently resourced to perform their tasks and their independence protected; and

4.6 **Individual employees as appropriate for their role and in order to enable them to comply with data protection law, are responsible for:**

4.6.1 ensuring they access or process personal data only where it is required as part of their role,

4.6.2 completing relevant data protection training, appropriate to their role,

4.6.3 following relevant advice, guidance and tools/methods provided by the Information Governance Group (and other relevant teams) depending on their role, regardless of whether access to and processing of personal data is through UKRI owned and managed systems, or through their own or a third party's systems and devices,

4.6.4 identifying new systems, processes (including changes to existing processes), contracts, agreements and other activities involving personal data that may require a data protection impact assessment, and cooperating with data protection advisors to support an assessment and implementation of recommendations to address risks as appropriate,

4.6.5 when processing personal data on behalf of UKRI, only using it as necessary for their role and not disclosing it unnecessarily or inappropriately,

4.6.6 recognising, reporting internally, and cooperating with any remedial work arising from personal data breaches, and,

4.6.7 recognising, reporting internally, and cooperating with the fulfilment of data subject rights requests when requested to do so by the Data Protection team.

5. Access to personal data

5.1 We uphold individuals' rights under data protection laws and allow them to exercise their rights over the personal data we hold about them. Our Privacy Notices[3] acknowledges these rights, explains how individuals can exercise them,

[3] UKRI Privacy Notice (https://www.ukri.org/about-us/privacy-notice/), and where relevant additional privacy policies.

where rights are absolute and may depend on the circumstances. All data subjects (including employees, research and innovation funding applicants and others who interact with UKRI) are entitled to make a subject access request to ask UKRI whether it holds any personal data relating to them and, if so, to be given a description of and a copy of that personal data. Exemptions may apply in certain circumstances.

5.2 Subject Access Requests are co-ordinated by the Information Governance Group's Data Protection team.

6 Data sharing

6.1 Personal data, in any format, will not be shared with a third-party organisation without a valid agreement in place, or the consent of data subjects.

6.2 Personal data will not be transferred outside of the UK without appropriate safeguards. Safeguards and technical measures will be informed by an assessment of the level of protection for the rights and freedoms of the data subjects in relation to the processing activities.

7 Privacy by design

7.1 UKRI is committed to meeting the GDPR requirement to consider data privacy at the initial design stages of a project as well as throughout the lifecycle of the relevant data processing.

7.2 Data protection impact assessments are a key mechanism in ensuring privacy risks are considered at an early stage. Assessments may involve a two-stage process, with an initial assessment followed by an in-depth data protection impact assessment where necessary. Assessments are required for all processing activity, systems and policies involving new uses, or changes to the use of personal data. They allow an organisation to demonstrate to data subjects and regulators that the personal data will be handled responsibly and in ways that are compliant with relevant legislation.

8 Personal data incidents

8.1 Personal data incidents, including breaches and near misses, must be reported immediately. Incidents can be reported to incidents@ukri.org and to relevant local information security teams.

8.2 Incidents will be investigated in line with relevant policies and handling guidance which aims to assess risks to individual's rights and freedoms, mitigate consequences, and reduce the risk of future breaches. Where appropriate UKRI's Data Protection Officer will report breaches to the Information Commissioner's Office within the required 72 hours timescale.

9 Policy Benefits

9.1 This policy will benefit UKRI by; promoting transparency and accountability, and

fostering a data protection culture across the organisation,

9.2 ensuring compliance with the relevant data protection legislation,

9.3 ensuring employee confidence and compliance in their processing of personal data, being fully informed and aware of their responsibilities and obligations,

9.4 reducing the risk of financial penalties and reputational damage from non-compliance,

9.5 providing confidence to the UKRI community that their personal data is being well managed and ensuring data subjects know how they can access their data,

9.6 ensuring proper procedures are in place for the collection, processing, and management of personal data, including special category and criminal convictions data where applicable,

9.7 assisting in ensuring other organisations with whom UKRI shares personal data meet compliance requirements as set out in the relevant data protection legislation,

9.8 ensuring that any new systems being implemented that will hold personal data are assessed as to whether the system presents any risks, damage or impact to individuals, and that appropriate mitigating action is taken in compliance with this policy.

10 Compliance

10.1 Breaches of this policy will be investigated, and appropriate actions taken.

10.2 This policy will be regularly reviewed every two years by the Information Governance Group, or as necessary in response to relevant legislative changes. Trade Unions may request that the policy is reviewed.

11 Storage

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

Data Protection Policy annex 1 - Associated documents

1. Associated relevant legislation

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Data Protection, Privacy and Electronic Communications Regulations 2019
- Human Rights Act 1998 (Remedial Order 2020)
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Equality Act 2010

2. Associated UKRI policy and process

- UKRI Records Management Policy
- UKRI Retention Schedule
- UKRI Information Security Incident and Data Breach Handling Policy
- UKRI Information Security Event/Incident & Data Breach Handling Process
- Information Security Policy Framework