UK Research and Innovation

UKRI Acceptable Use Policy

Contents

Policy Statement 1

Management Statement 1

Conventions 1

1. Scope 1

2. Principles 2

3. Personal files, documents and emails 2

4. Unacceptable, forbidden activities and penalties 2

5. Compliance 3

6. Derogations 3

APPENDIX A. Related Policies and Standards 3

APPENDIX B. Definitions 4

APPENDIX C. Unacceptable and forbidden activities 4

APPENDIX D. Version Control 6

Policy Statement

The UKRI Acceptable Use Policy (AUP) describes the responsibilities and expected conduct for Authorised Users of UKRI's information systems, networks, and electronic devices. The policy is designed to maintain the integrity, confidentiality, and availability of organisational resources, and to outline appropriate behaviour when accessing these resources.

Management Statement

This policy is approved by the Strategy, Policy, and Standards sub-committee. It is managed by the UKRI Information Security Function.

Conventions

Throughout this policy, controls are written using '**shall**', '**shall not**' and '**should**'. Where these are present, they are defined as follows:

- Controls that use '**shall**' and '**shall not**' require mandatory compliance.
- Controls that use '**should**' are considered recommendations that will further enhance security and will be followed wherever possible.

1. Scope

1.1 The policy applies to any individual who accesses UKRI information, systems, networks, or devices, including UKRI employees and non-employees (referred to in this document as "Authorised Users"), including all persons engaged to represent or act on behalf of UKRI, or its affiliated organisations worldwide who access UKRI systems, services, facilities, data and information provided either directly or indirectly, whether accessed from a UKRI site or remotely. For this policy:

1.1.1 the use of the word ‘employee’ covers UKRI employees on permanent or fixed term contracts.

1.1.2 the term ‘non-UKRI employee’ covers individuals such as, non-executive directors, board, council and committee members, students not on UKRI contracts, contingent workers and other third parties who access UKRI services and information to provide services or support.

2. Principles

2.1 UKRI relies on its technology and communications facilities for business operations. Improper use can damage research, operations, and UKRI’s reputation.

2.2 Authorised Users **shall** comply with applicable laws, including the Data Protection Act 2018, GDPR, and UKRI's Information Security Policies.

2.3 Activities outside acceptable use (see Appendix C) may lead to a full investigation (see UKRI Code of Conduct and UKRI Counter Fraud and Bribery Policy). For non-UKRI employees, actions will be discussed with their employer or third party responsible for them and UKRI reserves the right to withdraw access to UKRI resources and, where appropriate, terminate the individual’s engagement with UKRI. UKRI will report suspected criminal activity where allegations are serious, plausible, and supported by reasonable grounds.

2.4 Non-UKRI employees **shall** be informed of policy principles and restrictions before accessing UKRI systems. This includes a statement on personal use, which may be more restrictive.

3. Personal files, documents and emails

3.1 Unauthorised access, use, or disclosure of personal information is prohibited.

3.2 UKRI employees, at management discretion, may use systems for reasonable personal use if personal use is brief, low-volume, incidental use of UKRI systems that does not disrupt work, incur cost, introduce risk, resemble routine personal activity, or risk HMRC tax liability.

3.3 Personal use **should** be limited to non-working time. Limited personal use during work hours is tolerated, but excessive use may lead to action under the UKRI Code of Conduct.

3.4 Consider these questions to determine personal use: Is it acceptable to the public? Is it an effective use of work time? Will it impact UKRI's work? Could it bring UKRI into disrepute?

Authorised users **should** judge personal use based on circumstances and seek guidance if in doubt. If doubt remains, avoid that personal use.

3.5 UKRI does not permit the sharing externally of non-work documents on its services.

3.6 Any access to personal information for business continuity will comply with the UKRI Monitoring and Interception Policy and data protection requirements, including exceptions where UKRI is the processor but not the controller.

3.7 UKRI information **shall** only be shared through UKRI-approved systems or secure collaboration channels. Where external systems are required for legitimate business purposes, Authorised Users must follow UKRI guidance on secure transfer and data protection.

4. Unacceptable, forbidden activities and penalties

4.1 This policy outlines acceptable use principles. Appendix C lists excluded activities, categorised as ‘Unacceptable’ and ‘Forbidden.’ Breaches of this policy, including those activities, will be investigated.

4.2 Illegal or inappropriate material **shall** be reported promptly through the appropriate UKRI reporting channels.

4.3 Suspected phishing, malicious emails, or spam that bypasses UKRI’s email security controls **shall** be reported promptly using the phishing reporting button in Outlook or by forwarding to phishing@ukri.org. Routine spam or unsolicited marketing emails do not need to be reported unless they appear suspicious, harmful, targeted, or otherwise meet UKRI’s security incident reporting criteria.

4.4 Accidental access to, or unsolicited receipt of, illegal, inappropriate, discriminatory, abusive, pornographic, obscene, offensive, defamatory, or otherwise harmful material **shall** be reported promptly through the UKRI security incident reporting channel. Authorised Users **shall** stop viewing or interacting with the material immediately, avoid forwarding or further distributing it unless instructed, and preserve relevant details to support triage.

4.5 Where the incident has local operational, line management, welfare, safeguarding, HR, or workplace conduct implications, Authorised Users **shall** also notify their line manager, local IT Service Desk, local security representative, or other relevant local route as appropriate. Local reporting does not replace the requirement to report through the UKRI security incident reporting channel.

4.6 Accidental access or unsolicited receipt will not normally be treated as misconduct where it is reported promptly and the Authorised User does not continue to view, store, forward, conceal, or otherwise misuse the material. UKRI Information Security will triage reported incidents and escalate to Information Governance, HR, Legal, Personnel Security, safeguarding, law enforcement, or other relevant functions where required

5. Compliance

5.1 Information Security Teams, UKRI Information Governance Team, Internal Audit, and/or approved third party assessors may conduct random assessments to ensure compliance with this policy without notice. The UKRI CISO will have oversight of these assurance and compliance checks. Any non-compliance with this policy **shall** be reported to the UKRI CISO or delegated security authority at the earliest opportunity for risk assessment and corrective action. Where non-compliance involves conduct or performance issues, investigations will follow the relevant HR processes. Non-compliance that presents an information security risk **shall** be recorded in the UKRI Risk Register for oversight and mitigation. Technical owners **shall** implement corrective actions within agreed timeframes. Where non-compliance involves conduct or performance issues, investigations will follow the relevant HR processes.

5.2 Where unintentional breaches are discovered, a specific action plan and timeframe **shall** be jointly agreed between the CISO, or delegated individual, and the system/service/information owner(s) responsible.

5.3 Any suspected or confirmed non-compliance **shall** require a fact-finding investigation in line with the HR policy suite.

6. Derogations

6.1 In some exceptional cases, a system or service may be granted a derogation from parts or all of this policy. This may be due to technical limitations, operational constraints, or other valid reasons. However, any derogation **shall** be supported by a robust risk assessment and approved by the UKRI CISO in consultation with the relevant risk owner and system owner.

6.2 Derogations are only valid for a stated duration and **shall** be reviewed regularly. To request a derogation, the system or service owner **shall** complete the derogation request form. The system or service owner **shall** comply with any additional security measures or controls that may be imposed to mitigate risk.

APPENDIX A. Related Policies and Standards

UKRI Policies can be found on the external UKRI web site and on The Source.

Relevant UK Government Security policies.

Joint Information Systems Committee (JISC) Acceptable Use Policy, as UKRI use the JANET network.

UKRI policies remain subject to internal governance and consultation. External policies referenced are for awareness and do not automatically amend UKRI policy.

APPENDIX B. Definitions

- All UKRI Information Security related definitions can be found on The Source.

APPENDIX C. Unacceptable and forbidden activities

C. 1 Examples of unacceptable activities:

i. Making your personal username and password (also known as a 'user account') available for other people to use on your behalf.

ii. Allowing other people to use your device under your own user account without supervision.

iii. Accessing information, systems or services without appropriate authorisation or using another's credentials.

iv. Failing to comply with the Government Mobile Device Management Policy.

v. Spending working time on personal use of the internet, email, social media, and other systems and services beyond brief, incidental use.

vi. Transmitting, downloading or storing any material such that it infringes the copyright of the owner.

vii. Purchasing goods or services for UKRI use or entering into any contract on behalf of UKRI without the necessary authority.

viii. Business advertising, trade sales, or use of UKRI systems, services or resources to promote, operate, or support a personal or external commercial business. This does not prevent limited, local, non-commercial colleague-to-colleague exchanges, giveaways, or one-off personal sales where permitted by local arrangements and where the activity is incidental, low-volume, does not disrupt work, and does not create security, legal, reputational, financial, tax, or conduct risks.

ix. Trading for profit, including purchasing goods with the sole or primary intention of reselling them for personal gain, or repeated use of UKRI systems, services or resources to sell goods or services.

x. Using electronic communication mechanisms, messaging applications, collaboration tools, or cloud-based services for UKRI business where their use has not been approved, locally authorised, or risk assessed for the relevant purpose, information type, and operational context. Non-standard communication methods required for operational continuity, emergency response, fieldwork, research collaboration, or site-specific coordination **shall** be used in line with local arrangements and UKRI information handling, security, records management, and data protection requirements.

xi. Using unauthorised external email accounts for UKRI business.

xii. Unauthorised or inappropriate forwarding, sharing, publishing, or redistribution of emails or email content where this would disclose UKRI information, personal data, confidential, commercially sensitive, restricted, or third-party information to recipients without a legitimate need to know.

xiii. Sending or forwarding chain emails.

xiv. Deliberately creating, storing or transmitting information which infringes the data protection registration of UKRI. Using UKRI's provided communication equipment to make unauthorised personal/non-business-related calls to premium rate or international numbers; or subscribing to premium rate text messaging services.

xv. Deliberately enabling or assisting unauthorised access to UKRI systems or data.

xvi. Knowingly allowing the use of UKRI systems, services and resources by unauthorised third parties.

xvii. Disabling, altering, bypassing or circumventing any measures put in place by UKRI to maintain the safe and secure operation of systems, services and information. This includes non-cooperation with investigations or audits.

xviii. Misrepresenting UKRI by unauthorised or inappropriate publishing. For example, blog posts, tweeting.

xix. Failing to follow UKRI requirements on how to protect, store, transmit, share and access information both within and outside UKRI.

xx. Failing to purchase and dispose of systems, services and information in line with UKRI policy.

xxi. Inappropriate messaging to large groups of people. For example, sending non-work-related emails to all staff, across an institute.

xxii. Use of the UKRI electronic communication mechanisms e.g email or social media, to harass, threaten, or intimidate others, solicit or promote personal or personal commercial activities, or post offensive or inappropriate content.

xxiii. Where UKRI networks are being used to access another network e.g JISCs JANET network or CERN network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of UKRI's networks.

xxiv. Incurring excessive or inappropriate mobile data/voice charges using UKRI provided mobile communication equipment (e.g. extra charges incurred through non-essential use of a mobile devices Sat Nav capability or through non-essential use when travelling overseas).

NOTE: UKRI Tenant organisations and some third parties may be permitted these activities if they are explicitly included in appropriate tenancy agreements or equivalent.

C. 2 Examples of forbidden activities:

i. Using another person's log on details (username and password).

ii. Attempting to gain or facilitate unauthorised access to a computer system, service or information.

iii. Attempting to or deliberately corrupting, destroying or denying access to another user's email, data files, information, system or service.

iv. Deliberately altering, bypassing or circumventing UKRI Policy and technical measures on how to protect, store, transmit, share and access information both within and outside UKRI.

v. Deliberately accessing, viewing, receiving, downloading, sending or storing material:

   a. with pornographic, offensive, obscene or indecent content;

   b. related to criminal skills or terrorist activities;

   c. that promote or encourage discrimination, racism or intolerance;

   d. that facilitates illegal activity in the UK or the host country;

   e. that is illegal in the UK or the host country;

   f. that is defamatory, threatening, harassing, offensive or abusive;

   g. that will, or is likely to, bring UKRI, its staff or partners into disrepute;

   h. that is known or reasonably suspected to be infected with a virus, worm, Trojan, malicious software, malicious code, or other harmful payload, unless formally authorised for legitimate cyber security, forensic investigation, incident response, malware analysis, research, or evidence-handling purposes and handled in accordance with approved procedures and appropriate technical controls;

   i. that infringes the privacy and data protection rights of individuals;

   j. that could endanger the health and safety of any other individual.

APPENDIX D. Version Control

Version Number	Status	Revision Date	Summary of Changes
1.0		13/12/17	Approved by D&T Project Board
2.1		23/4/24	Review comments added
2.2		7/8/25	New style
3.0	Approved	23/6/26	Strategy, Policy and Standards Sub-Committee approved

Date of next review: June 2028