UK Research and Innovation

Acceptable Use Policy

Contents:

Appendices:

Policy Statement

UKRI Information and Communication Technology (ICT) systems, services and facilities are provided to enable employees and other authorised individuals to perform their jobs effectively and efficiently. All normal use of these systems within an individual's authority to act in pursuit of UKRI business, is allowed. Illegal activity is not allowed.

The purpose of this Policy is to identify proper usage and behaviour of individuals using UKRI/establishment ICT systems and services. The overall aim of this Policy is to protect the rights and privacy of all employees, and the integrity and reputation of UKRI. It should be read in conjunction with all the Policies and Standards on the UKRI Intranet and within each Council.

Some limited and reasonable personal use of UKRI's ICT systems and services by employees is allowed provided that it is not excessive and does not:

- interfere with normal work or the work of others

- involve more than minimal amounts of working time
- involve UKRI in unauthorised expense
- expose UKRI to legal action or risk bringing UKRI into disrepute
- relate to running a private business.

This Acceptable Use Policy (AUP) applies to all individuals who access UKRI-provided ICT systems, services and equipment, irrespective of whether they are direct employees of UKRI. The Policy sets the minimum common standards of ICT acceptable use. Where additional organisational, institute, local, site or project standards of acceptable use are set, these must be consistent with the minimum standards set by this Policy and documented separately.

Breaches of the Policy will be dealt with under the UKRI Managing Performance and Conduct Policy and/or other organisational Policies or legal processes which may apply. Unacceptable and forbidden activities are set out in Appendix A.

Sensitive or personal information must be appropriately protected in line with UKRI Policy, such as the UKRI Data Protection Policy and other associated Policies and Guidance.

Whether a worker is deemed to be a worker or employee is not always clear under employment legislation. In cases where managers or individuals have any doubt as to whether this AUP should apply, assume that it does and then seek advice from the UKRI HR Team.

References

UKRI Code of Conduct Policy
UKRI Managing Performance and Conduct Policy
UKRI Counter Fraud and Bribery Policy
UKRI Data Protection Policy
UKRI Classification Principles and Standards
UKRI Personal Use of Social Media
UKRI Counter Fraud and Bribery Policy
UKRI Infohub
UKRI Overseas IT Equipment Travel Policy
UKRI Overseas IT Equipment Travel Standards
UKRI Travel to China on Official Business Standards
Jisc Acceptable Use Policy
Government Security Classifications

Version Number	Status	Revision Date	Summary of Changes
0.1		11 August 2017	Draft Policy created
0.2		17 August 2017	Revision post WS3 board members review
0.3		31 August 2017	Revision post ISOG review
0.4		04 September 2017	Revision post project team review

0.5		30 September 2017	Updates to sections & scope
0.6		14 November 2017	Revision post WS3 board members review
0.7		26 November 2017	Formatting revision
0.8		30 November 2017	Post consultation comments
0.9		06 December 2017	Amendments post WS3 Project Board
1.0		13 December 2017	Approved by D&T Project Board
1.0	Draft	26 February 2018	Revision following comments from TUS
1.1		20 March 2018	Updated ‘Local IT Service Desk’ to ‘UKRI IT Help Desks’
1.2		26 June 2018	Further revision following additional TUS comments
1.3		03 January 2020	Head of Information Security update
1.4		29 February 2020	Stakeholders review
1.5	Complete	01 April 2020	Rebranded as UKRI

Related Documents

Version Number	Document	Comments

Document Review & Approval

Name	Version	Signature/Email Confirmation	Date
WS3 Project Board	0.9	See minutes	5/12/2017
D&T Project Board	1.0	See minutes	13/12/2017
Trade Union	1.5	Email confirmation	15/5/2020
UKRI Security Committee	2.0	See minutes	5/6/2020

Document Circulation/Readership

The intended circulation/readership for this document are as follows:

- All authorised users of UKRI information and information systems, both those who are members of UKRI staff and those who are not (e.g. UKRI employees, contractors, facility users, collaborators, temporary staff and secondees).

1. Principles

1.1 The Policy applies to all authorised users of UKRI information and information systems, both those who are members of UKRI staff and those who are not (e.g. UKRI employees, contractors, facility users, collaborators, temporary staff and secondees)

1.2 It applies to authorised users accessing information, information systems and software in all forms, independent of the medium on which they are held (e.g. physical, electronic, file, etc.), the form which they take (e.g. text, pictures, software, programs, databases, information systems, audio, video, internet etc.) or whether accessed from a UKRI site or remotely.

1.3 UKRI relies on its computer and communications facilities to carry out its business. All these facilities can be put at risk through improper or ill-informed use and result in consequences which may be damaging to individuals and their research, UKRI operations, the UKRI community and its reputation.

1.4 The Policy aims to provide clear information to all authorised users concerning the use of UKRI information, information systems and software in all forms. It provides a framework to:

1.4.1 Enable employees to use UKRI facilities securely and with confidence;

1.4.2 Help maintain the security, integrity and performance of UKRI systems and services;

1.4.3 Minimise both the UKRI and individual users' exposure to possible legal action arising from unauthorised use of the systems and services;

1.4.4 Minimise UKRI and individual users' exposure to unauthorised, excessive or inappropriate expense through business related activities;

1.4.5 Help ensure that UKRI can demonstrate effective and appropriate use of publicly funded resources; and

1.4.6 Set the minimum standard for acceptable use across all UKRI systems and services.

1.5 It is UKRI's responsibility to ensure that all authorised users have access to this Policy. It is each authorised user's responsibility to read, make themselves fully familiar with, and abide by this Policy, the Joint Information Systems Committee (JISC) Acceptable Use Policy and any relevant local Policies.

1.6 Sensitive or personal information must be appropriately protected in accordance to the UKRI Classification Principles and Standards and in line with the Government Security Classification Scheme. Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats.

1.7 Any activity that falls outside acceptable use (see Appendix A) may result in disciplinary action (see the UKRI Managing Performance and Conduct Policy). Where the activity is deemed to amount to gross misconduct, this will normally lead to summary dismissal. Where relevant, the UKRI Counter Fraud and Bribery Policy may also be invoked. For non-employees any action will be discussed with the individual's management (as appropriate); this may include being denied access to UKRI/establishment sites. Any suspected criminal activity will be reported to the police.

1.8 Non-employees will be made aware of the principles of the Policy, and any restrictions/guidance, before they have access to UKRI/establishment systems, services and information. This will include a statement on personal use (which should be in line with the restrictions placed on UKRI staff but may be more restrictive if required).

2. Monitoring

2.1 UKRI reserves the right to monitor communications.

2.2 UKRI employs monitoring techniques on its systems and services, including email and Internet access, to enable the continuous improvement of services, detection of illegal activity, and to ensure that these facilities are not being misused.

2.3 Monitoring is limited to the minimum data to fulfil the purpose of the monitoring activity (e.g. security, performance tuning) and will not normally include the gathering of personal information. Processing is most often through the use of automated tools and access to the logs is restricted to authorised personnel, such as Information Security Teams or associated system admins. Investigations of suspected abuse are only conducted when authorised by HR and the SIRO (or a person with delegated security responsibility) and are carried out by appropriately trained staff.

2.4 UKRI subscribes or uses services provided by third parties (e.g. Microsoft, UKSBS Ltd). These parties may also monitor the access and use of those services to protect them from unauthorised access, improve their service offerings or to determine payment charges.

2.5 Since UKRI owns and is liable for data on its systems and services, it reserves the right, as part of any investigation, to inspect the contents of any emails or any other form of communications that are sent or received and of Internet sites accessed, for compliance with this Policy. This will be done where the volume of traffic or the amount of material being downloaded or uploaded is excessive or there are grounds to suspect that use is for 'unacceptable' or 'forbidden' activities (see Appendix A).

2.6 Monitoring/investigations of individuals' use of the UKRI's communications systems may also happen in the following circumstances:

2.6.1 To detect or prevent crime including detecting unauthorised use of systems and/or inappropriate or illegal activity, as well as protecting against malware, hackers and fraud;

2.6.2 To assist in maintaining the security, performance, integrity and availability of the systems, services and information;

2.6.3 To provide evidence e.g. of a commercial transaction, to establish regulatory compliance, audit, debt recovery, dispute resolution.

2.7 Exceptionally, where there is a defined and valid reason for doing so, the inspection may include items that are non-work related or marked ‘private’ or ‘personal’ for example.

2.8 An individual’s email and voicemail accounts may also be accessed by management when the individual is absent from work to ensure official business matters can be effectively dealt with. Authorisation for such access is given by the UKRI Head of Information Security, SIRO or equivalent Director. Management will make a reasonable attempt to inform and obtain agreement from the user prior to this occurring.

2.9 Where monitoring is used, only UKRI staff trained in data protection compliance will investigate the recorded data. Confidentiality will be ensured for all investigations involving personal data, except to the extent that wider disclosure is required to follow up breaches, to comply with court orders or to facilitate criminal investigation. Logged data will not normally be retained for more than two years unless required by regulatory compliance. Please refer to the UKRI Data Protection Policy.

2.10 In addition, members of the UKRI Information Security Team, UKRI IT Help Desks, Information Security representatives and Network Security Groups will conduct random audits on the security of UKRI’s systems, services and information. These audits include examination of a small, randomly selected set of user devices and server systems. The audit checks that these systems have correctly licensed software, appropriately patched, do not contain inappropriate material and have not been used to access or view inappropriate material that may violate this Policy.

2.11 Where monitoring reveals instances of suspected misuse of the systems, services or information (e.g. where pornography or other inappropriate material is found, or where substantial time-wasting or other unacceptable/forbidden use is found), these will be investigated and pursued through normal disciplinary procedures and may result in dismissal.

3. Approval/authorisation

3.1 Prior to commitment or use of chargeable and non-chargeable systems and services, such as work mobile phone use, staff must ensure they have appropriate authorisation and manage such usage within the agreed limits. Unapproved or excessive expenditure will be subject to investigation. Staff should always endeavour to minimise costs by using the most appropriate tools and services.

4. Personal files, documents and emails

4.1 To help safeguard their privacy it is suggested that employees mark any personal emails they send with the word ‘Private’ or ‘Personal’ in the “subject” line and ask those they correspond with to similarly mark any personal emails being sent.

4.2 Where personal (non-UKRI) information is stored on UKRI services such as O365 or file servers, they should be clearly marked as to identify them as not work related and saved only in locations where they can only be accessed by the individual (Note: authorised personnel, such as system admins, will still have access to these areas as part of the overall maintenance and support of system or service). UKRI does not permit the sharing of non-work information on its services. Whilst UKRI takes steps to ensure the security of all information held on its services, it is not liable for such information stored on its systems should it be lost, destroyed or accessed inappropriately.

4.3 Where possible, those staff responsible for monitoring or inspecting the systems and services will respect emails and folders which are marked ‘Personal’ or ‘Private’.

4.4 Access to personal information areas to ensure business continuity, for instance during unexpected absence, will respect where possible items clearly marked as private or personal.

4.5 At management discretion, UKRI employees are allowed limited and reasonable personal use of UKRI systems and services provided that such use does not:

4.5.1 interfere with their (or others’) work, and/or;

4.5.2 involve more than minimal amounts of working time;

4.5.3 incur any unauthorised expense for UKRI and/or tie up a significant amount of resource.

4.6 Personal use should be limited to non-working time e.g. at lunchtime, before/after normal working hours, or when “clocked out” for members of flexi schemes. Very limited, occasional personal use during normal working time will be tolerated (e.g. to respond briefly to an incoming personal email or telephone call or to deal with a non-work-related emergency). However, spending significant amounts of time making personal use of the internet, email, communication equipment, etc. is not acceptable and may lead to disciplinary action.

4.7 Before undertaking personal use, employees should ask themselves the following questions:

4.7.1 Would the actions be considered unacceptable if viewed by a member of the public?

4.7.2 Would managers, auditors or others in similar positions call into question the cost effectiveness of use of work time or use of UKRI systems and services?

4.7.3 Will personal use have a negative impact upon the work of colleagues (e.g. in terms of their motivation and morale)?

4.7.4 Could personal use bring UKRI directly or indirectly into disrepute?

4.8 Personal use should not be undertaken if the answer to any of these questions is yes.

4.9 Responsibility for ensuring that any personal use is acceptable rests with the individual. Employees should seek guidance from their line manager if they have any doubts concerning the acceptability of their personal use. If any doubt still remains, then that form of personal use should not be undertaken.

5. Social media

5.1 UKRI recognises the value of using social media in work related communication. It can be an effective way to respond to queries, keep stakeholders informed, and track and respond to mentions of UKRI. Employees should have line manager approval before using social media for work related communication and must read and comply with any local rules before using social media for UKRI related work.

5.2 Personal use of social media is covered in the UKRI Personal Use of Social Media Policy.

6. Overseas travel

6.1 Overseas travel can form part of a member of staff's role. However, precautions must be taken to ensure that any use of digital systems overseas does not have the potential to place UKRI systems or information at risk; including personal devices that have access to UKRI information.

6.2. Staff travelling overseas for work purposes (or for personal reasons such as a holiday) with UKRI provided digital equipment must contact their local IT Service Desk who will work with the UKRI security professionals to ensure any risks are appropriately managed, which may include separate or specialist equipment to be used in those locations. Further information can be found in the UKRI Travel Policies and Standards.

7. Exceptions

7.1 The nature of some forms of work might seem to contravene what would normally be considered appropriate use, for example the study of some medical research. Where these are necessary, they must be restricted to specific approved work identified as necessary for completion of that activity and security professionals consulted who will provide guidance appropriate to the activity and record the exception.

8. Related policies and procedures

8.1 For those sites connected to the JANET network, users should ensure they also comply with the Joint Information Systems Committee (JISC) Acceptable Use Policy.

8.2. UKRI staff must familiarise themselves with all organisational, Institute/Centre, local, site or project Information Security Policies, Standards, best practice and guidance. These can be found on the UKRI InfoHub or local Intranet.

9. Policy review

9.1. This Policy will be reviewed every 2 years to incorporate any legislation or regulatory changes. The Trade Union Side may also request that this Policy is reviewed.

A1. Unacceptable and Forbidden Activities and Penalties

A1.1 This Policy sets the common minimum standards for the acceptable use of systems, services and information. The activities below are those of which are specifically excluded; the list is not comprehensive. The list is divided into two sections (“Unacceptable” and “Forbidden”) to help highlight the most serious activities. The consequences of undertaking any of the activities listed below (or other instances) will be determined through the normal disciplinary procedures. All such activities are considered to be serious and are likely to be viewed as misconduct. It is likely that undertaking a forbidden activity, or repeating an unacceptable activity, will be viewed as gross misconduct.

A1.2 Unsolicited receipt of discriminatory, abusive, pornographic, obscene, illegal, offensive or defamatory messages (e.g. email SPAM/text messages) will not be treated as a disciplinary offence. With the exception of illegal material, anyone who receives such material should follow local guidance on how to report it to the appropriate person. An employee who accidentally accesses a pornographic or other inappropriate web page should report the matter to their line manager. No disciplinary action will be taken in such cases. If the line manager is unavailable, the employee should contact the UKRI Information Security Team or their local IT Service Desk.

A1.3 Anyone accidentally viewing what they believe is illegal material (e.g. child pornography) must immediately stop what they are doing, take a note of where they found the illegal material and close the software application displaying the material; this includes email. The individual must not view the illegal material again and must take appropriate measures to ensure that others cannot view the material. They must immediately inform their line manager and the UKRI Information Security Team, who will decide how to proceed. It may be a criminal offence to continue to view, allow others to view, or not to report some illegal material.

A1.3.1 Unacceptable activities

A1.3.1.1 Spending more than reasonable amounts of working time making personal use of the internet, email, social media and other systems and services.

A1.3.1.2 Transmitting, downloading or storing any material such that it infringes the copyright of the owner.

A1.3.1.3 Purchasing goods or services or entering into any contract on behalf of UKRI without the necessary authority.

A1.3.1.4 Business advertising or trade sales.

A1.3.1.5 Trading, i.e. sale of any goods purchased with the sole intention of making a profit.

A1.3.1.6 Using an unauthorised electronic communication mechanism or cloud-based service.

A1.3.1.7 Using unauthorised external email accounts for UKRI business.

A1.3.1.8 Unauthorised redistribution of email.

A1.3.1.9 Sending or forwarding chain emails.

A1.3.1.10 Making your personal username and password (also known as a 'user account') available for other people to use on your behalf.

A1.3.1.11 Allowing other people to use your device under your own user account without supervision. Leaving your computer open when you are away from your desk increases the risk of this happening.

A1.3.1.12 Accessing information, systems or services without appropriate authorisation or using another's credentials.

A1.3.1.13 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.

A1.3.1.14 Knowingly allowing the use of UKRI system, services and resources by unauthorised third parties.

A1.3.1.15 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.

A1.3.1.16 Misrepresenting UKRI by unauthorised or inappropriate publishing. For example, blog posts, tweeting etc.

A1.3.1.17 Failing to follow UKRI requirements on how to protect, store, transmit, share and access information both within and outside UKRI.

A1.3.1.18 Failing to purchase and dispose of systems, services and information in line with UKRI Policy.

A1.3.1.19 Inappropriate messaging to large groups of users. For example, sending non-work-related emails to all staff, across an institute etc.

A1.3.1.20 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 device such as a Sat Nav or through non-essential use when travelling overseas).

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

A1.3.2 Forbidden activities

A1.3.2.1 Using another person’s log on details (username and password).

A1.3.2.2 Attempting to gain or facilitate unauthorised access to a computer system, service or information.

A1.3.2.3 Attempting to or deliberately corrupting, destroying or denying access to another user’s email, data files, information, system or service.

A1.3.2.4 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.

A1.3.2.5 Deliberately accessing, viewing, receiving, downloading, sending or storing material:

A1.3.2.5.1 with pornographic, offensive, obscene or indecent content;

A1.3.2.5.2 related to criminal skills or terrorist activities;

A1.3.2.5.3 that promote or encourage discrimination, racism or intolerance;

A1.3.2.5.4 that facilitates illegal activity in the UK or the host country;

A1.3.2.5.5 that is illegal in the UK or the host country;

A1.3.2.5.6 that is defamatory, threatening, harassing, offensive or abusive;

A1.3.2.5.7 that will, or is likely to, bring UKRI, its staff or partners into disrepute;

A1.3.2.5.8 that is known to be infected with a virus, worm, Trojan or any form of malicious software or code;

A1.3.2.5.9 that infringes the privacy and data protection rights of individuals;

A1.3.2.5.10 that could endanger the health and safety of any other individual.