RESEARCH COUNCIL ACCEPTABLE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SYSTEMS AND SERVICES POLICY

Content

Policy Statement

The Research Council's 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 in pursuit of individual Research Council business within an employee's authority to act is allowed. Illegal activity is not allowed.

The purpose of this policy is to identify proper usage and behaviour for Research Council/establishment ICT systems with the overall aim of protecting the rights and privacy of all employees, and the integrity and reputation of the Research Council. It should be read in conjunction with the Personal Use of Social Media Policy.

Some limited and reasonable personal use of the Research Council's ICT systems 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 the Research Council in significant expense
- expose the Research Council to legal action or risk bringing the Research Council into disrepute
- relate to running a private business.

This policy applies to all employees of the Research Council. The principles of the policy will also be applied, as far as is reasonably practicable, to non-employees working at Research Council/establishment locations and making use of Research Council/establishment ICT systems (e.g. facilities users, Panel Members, Council members, contractors, visitors).

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.

Breaches of the policy will be dealt with under the Disciplinary Policy and/or, as appropriate, Fraud Policy. Examples of unacceptable activities are set out in Annex A.

Sensitive or personal information must be appropriately protected in line with Government and Research Council policy.

The UK Shared Business Services (UK SBS) provides HR services across the Research Councils. However some employees are deployed at establishments/ facilities/ships that do not access services from SBS. In these cases reference to the SBS or System (Employee Self Service) will not apply and employees should refer to their Research Council HR team for assistance.

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 Acceptable Use Policy should apply, assume that it does and then seek advice from the Research Council HR team.

RESEARCH COUNCIL ACCEPTABLE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY SYSTEMS AND SERVICES POLICY

1. Principles

1.1 The Research Council 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, the Research Council community and to reputations.

1.2 The policy aims to provide clear guidance to all employees concerning the use of Research Council computer and communications facilities. It provides a framework to

- enable employees to use Research Council facilities with security and confidence,
- help maintain the security, integrity and performance of Research Council ICT systems;
- minimise both the Research Council and individual users' exposure to possible legal action arising from unauthorised use of the ICT systems;
- help ensure that the Research Council can demonstrate effective and appropriate use of publicly funded resources; and
- set the minimum standard for acceptable use across all Research Council ICT systems.

1.3 It is the Research Council's responsibility to ensure that employees have access to this policy, both on joining and during their employment. It is each employee's responsibility to read, make themselves fully familiar with, and abide by the policy, JANET Acceptable Use Policy (see 5.1) and any relevant local policies.

1.4 The policy covers use of all ICT systems and facilities provided either directly or indirectly by the Research Councils or used to conduct Research Council business, whether accessed from a Research Council site or remotely, in particular:

the Internet

- Electronic communications (in all forms) for example e-mail, social media used for business related communication, etc.
- electronic bulletin boards and social media
- file sharing by whatever means
- Computing devices (e.g. Desktops, laptops, printers, mobile devices etc.) and servers
- Communications equipment (e.g. telephones (land-line and mobiles), faxes and video conferencing)

1.5 Sensitive or personal information must be appropriately protected 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. There are three levels of classification OFFICIAL, SECRET and TOP SECRET.

1.6 The classifications of OFFICIAL, SECRET and TOP SECRET should be used in place of any and all of the previous protective markings.

1.7 All information that is created, processed, generated, stored or shared within the Councils is, at a minimum, OFFICIAL. The vast majority of our information falls under the OFFICIAL classification and does not need to be marked. OFFICIAL-SENSITIVE information is of a particularly sensitive nature and must be clearly marked. This classification should only be used in limited circumstances where there is a clear and justifiable requirement to reinforce the "need to know." OFFICIAL-SENSITIVE descriptors may also be added to identify the sensitivity of the information. Only three descriptors can be used with the SENSITIVE caveat and these are PERSONAL; COMMERCIAL; and LOCALLY SENSITIVE (LOCSEN). No other descriptors are to be used.

1.8 Further information about the scheme can be found on the Government Security Classifications page.

1.9 Any activity that falls outside acceptable use (see Annex A) may result in disciplinary action (see the Research Council's Disciplinary Policy). Where the activity is deemed to amount to gross misconduct, this will normally lead to summary dismissal. Where relevant the Council Fraud 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 Research Council/establishment sites. Any suspected illegal action will be reported to the police.

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

2. Monitoring

2.1 Monitoring Statement

2.1.1 The Research Council reserves the right to monitor communications.

2.1.2 The Research Council employs monitoring techniques on its ICT systems and services, including e-mail and Internet access, to enable usage trends to be identified and to ensure that these facilities are not being misused.

2.1.3 Monitoring is limited, as far as practicable, to the recording and analysis of network traffic data. To this end, the Research Council keeps logs of: calls made on communications equipment such as telephones and fax machine; emails sent by e-mail address; internet sites visited by computer system address. In some cases, this means that the identity of the individuals involved in the communication is readily available. These logs are not routinely monitored on a continuous basis but spot-checks are carried out from time to time to help ensure compliance with this policy. Further authorised investigations may be necessary where there is reasonable suspicion of misuse of facilities.

2.1.4 Since the Research Council owns and is liable for data held on its communications equipment and systems, it reserves the right, as part of any investigations, to inspect the contents of any e-mails or any other form of communications that are sent or received and of Internet sites accessed, for compliance with this policy. This will only be done where the volume of traffic or the amount of material being downloaded is excessive, or there are grounds to suspect that use is for 'unacceptable' or 'forbidden' activities (see examples in Annex A).

2.1.5 Exceptionally, where there is a defined and valid reason for doing so, the inspection may include items marked 'private' or 'personal'. An individual's e-mail and voice-mail 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 Senior Information Risk Owner or equivalent Director. Management will make a reasonable attempt to inform and obtain agreement from the user prior to this occurring.

2.1.6 Monitoring/investigations of individuals' use of the Research Council's communications systems may also happen in the following circumstances:

To detect or prevent crime including detecting unauthorised use of systems, protecting against viruses and hackers and fraud investigation

To assist in maintaining the security, performance, integrity and availability of the ICT systems, services and facilities.

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

2.1.7 Where monitoring is used, only Research Council 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 one year unless required by regulatory compliance Please refer to the Research Council Policy on Data Protection available from Knowledgebase or by contacting the Research Council HR Team.

2.1.8 In addition, members of the local IT Service Desk, Information Security representatives, Security Teams and Network Security Groups will conduct random audits on the security of the Research Council's ICT systems. 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, do not contain inappropriate material and have not been used to access or view inappropriate material that may violate this Policy.

2.1.9 Where monitoring reveals instances of suspected misuse of the ICT systems (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 through normal disciplinary procedures and may result in dismissal.

2.2 Personal files, documents and e-mails

2.2.1 To help safeguard their privacy it is suggested that employees mark any personal e-mails they send with the word 'Private' in the "subject" line and to ask those they correspond with to similarly mark any personal e-mails being sent.

2.2.2 Personal files, documents and e-mails can be stored in ICT systems provided they are in a folder clearly marked as 'Personal' or 'Private'. Note that corporate electronic document or record management facilities (ERMS etc.) do not include a facility for personal data so should not be used for this.

2.2.3 Where possible, those staff responsible for monitoring or inspecting the IT and communications systems will respect e-mails and folders which are marked 'Personal' or 'Private'.

2.2.4 In cases where misuse is suspected, all appropriate ICT systems, including emails and folders marked 'Personal' or 'Private', will be checked to establish whether there may be a case to answer.

3. Private/Personal use of ICT systems, services and facilities

3.1 At management discretion, Research Council employees are allowed **limited and reasonable** personal use of Council ICT systems, services and facilities provided that such use does not:

interfere with their (or others') work; and/or

involve more than minimal amounts of working time;

incur any significant expense for the Research Council and/or tie up a significant amount of resource.

3.2 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 e-mail or telephone call or to deal with a non-work related emergency). However, spending significant amounts of time making personal use of the internet, e-mail, communication equipment, etc. is not acceptable and may lead to disciplinary action.

3.3 Before undertaking personal use, employees should ask themselves the following questions.

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

Would managers, auditors or others in similar positions call into question the cost effectiveness of use of work time or use of the Research Council ICT systems and facilities?

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

Could personal use bring the Research Council directly or indirectly into disrepute?

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

3.4 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.

4. Social Media

4.1 The Research Council 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 the Research Council. 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 Research Council related work.

4.2 Personal use of social media is covered in a separate policy.

5. Related Policies and Procedures

5.1 Where an external network connection is provided as part of the Joint Academic Network (JANET), the JANET Acceptable Use Policy applies.

5.2 Employees must familiarise themselves with the Research Council's data protection policies, relevant organisational, institute, local, site or project Information Security Policy, standards, best practice and guidance.

6. Policy Review

6.1 This policy will be regularly reviewed to incorporate any legislation or regulatory changes. The TUS may request that a policy is reviewed.

Amendment history

Version	Date	Comments/Changes
V2.0	01 July 2014	New Government Security Classification Scheme covered (para 1.5 – 1.8)
V2.0	01 July 2014	Clarification provided for personal emails (para 2.2.1)
V3.0	01 November 2014	Details provided at 2.1.7 on where to obtain Data Protection Policy

ANNEX A

Unacceptable Activities and Penalties

This policy sets the common minimum standards for the acceptable use of ICT systems and services. Set out below are examples of activities and uses which are specifically excluded. The list is not comprehensive and 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.

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 their local IT Security Officer.

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 inform their line manager and the relevant IT Security Officer, 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.

Examples of Unacceptable Activities

- Spending more than permitted amounts of working time making personal use of the internet, e-mail, and other ICT Systems and services.
- Transmitting, downloading or storing any material such that this infringes the copyright of the owner.
- Purchasing goods or services or entering into any contract via the Internet or any other ICT system on behalf of the Research Council without the necessary authority.
- Business advertisements or trade sales*.
- Trading, i.e. sale of any goods purchased with the sole intention of making a profit*.
- Using an unauthorised electronic communication mechanism or cloud based service.
- Using unauthorised external email accounts for Council businesses.
- Unauthorised redistribution of email.
- Sending or forwarding chain emails.
- Making your personal user name and password (also known as a 'user account') available for other people to use on your behalf.
- Accessing another individual's data, ICT systems or service without appropriate authorisation.
- Deliberately creating, storing or transmitting information which infringes the data protection registration of the Research Council.

- Using the Research Council'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.
- Knowingly allowing the use of Research Council ICT resources (for example Internet bandwidth) by unauthorised third parties*.
- Disabling, altering bypassing or circumventing any measures put in place by the Research Council to maintain the safe and secure operation of ICT systems and services. This includes non-cooperation with investigations or audits.
- Misrepresenting the Research Council by unauthorised or inappropriate publishing. For example blog posts, tweeting etc.
- Failing to follow Research Council advice on how to protect, store, transmit, share and access sensitive information both within and outside the Research Council.
- Failing to purchase and dispose of ICT systems and services in line with Research Council policy.
- Inappropriate messaging to large groups of users. For example, sending e-mails to all staff, across an institute etc.

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

Forbidden activities

- Using another person's identity so as to appear to be someone else.
- Attempting to gain or facilitate unauthorised access to a computer system or information.
- Attempting to or deliberately corrupting, destroying or denying access to another user's e-mail, data files, information, ICT system or service.
- Deliberately altering, bypassing or circumventing Research Council advice on how to protect, store, transmit, share and access sensitive information both within and outside the Research Council
- Deliberately accessing, viewing, receiving, downloading, sending or storing material:
    - with pornographic, offensive, obscene or indecent content;
    - related to criminal skills or terrorist activities;
    - that promote or encourage discrimination, racism or intolerance;
    - that facilitates illegal activity in the UK or the host country;
    - that is illegal in the UK or the host country;
    - that is defamatory, threatening, harassing, offensive or abusive;
    - that will, or is likely to, bring the Research Council, its staff or Council members into disrepute;
    - that is known to be infected with a virus, worm, Trojan or any form of malicious software or code;
    - that infringes the privacy and data protection rights of individuals;
    - that could endanger the health and safety of any other individual.