RESEARCH COUNCIL PERSONAL USE OF SOCIAL MEDIA POLICY

CONTENT

Policy statement

1. **Principles**
2. **Definition of terms**
3. **Personal use of social media networking sites**
4. **Personal conduct**
5. **Monitoring of use**
6. **Security issues**
7. **Consequences of misuse**
8. **Policy review**
9. **Amendment history**

Policy statement

The Research Council recognises the organisational value of using social media websites in business 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. You may need line management approval, and to read and comply with any local rules before using social media tools and technologies for Research Council associated work.

The purpose of this policy is broader than use of social media at work; it is to identify proper usage and behaviour for social media applications used on a personal basis irrespective of location, 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 Research Council's policy on Acceptable Use of Computer Facilities and Communications Systems.

This policy applies to all employees of the Research Council. This includes those employed on temporary contracts and includes Visiting Workers, students or those workers provided by a third party agency.

This policy is agreed with the Trade Union Side and complies with legislation.

The UK Shared Business Services Ltd (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 references 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 the Personal Use of Social Media Policy should apply, advice should be sought from the Research Council HR team.

1. Principles

1.1 Employees are fully responsible for their own actions and the consequences of their actions when accessing these sites when at work and at all other times.

1.2 Content posted on social media websites has the same legal status as written documents.

1.3 When assessing the impact on the reputation and integrity of the Research Council, the content of material posted on social media sites is the primary consideration; the location from which the material was posted is secondary to this but is nevertheless significant.

1.4 As specified in the Acceptable Use of Computer Facilities and Communications Systems Policy (*link)*, the Research Council generally permits employees limited and reasonable use of computing facilities for personal use during non-working time, for example at lunch time. This includes access to social media networking sites.

1.5 The Research Council reserves the right to restrict access to social media networking websites using the Research Council's computer facilities.

2. Definition of terms

2.1 Social media is the term commonly used for websites which allow people to interact with each other, for example, by sharing information, opinions, knowledge and interests. Social media website content can include text, images, audio, and video.

2.2 Examples of social media websites include:

- Social networking websites – Facebook
- Wikis - Wikipedia
- Video sharing - YouTube
- Presence apps – Twitter

3. Personal conduct

3.1 The Research Council must ensure that confidentiality and organisational reputation are protected. However it recognises that individuals use social networking websites on a personal basis. Where an employee has identified themselves as working for the Research Council they are expected to:

- avoid discussing Research Council business
- direct work related enquiries to appropriate business channels
- take care not to allow their interaction on these websites to damage working relationships between members of staff and other stakeholders
- not infer a Research Council relationship with other organisations.

3.2 Any communications that employees make in a personal capacity through social media must not:

- Do anything that could be considered discriminatory against, or bullying or harassment of colleagues, for example by making offensive or derogatory comments relating to age, sex, race, religion or belief, sexual orientation, disability, marriage or civil partnership, pregnancy or maternity, or gender reassignment; using social media to bully another employee; posting images that are discriminatory or offensive (or links to such content)

- Bring the organisation into disrepute, for example by making defamatory statements about the Research Council, its employees or stakeholders; criticising colleagues or stakeholders
- Breach confidentiality, for example by giving away confidential information about a colleague or the organisation.

4. Monitoring and investigation of use and misuse

4.1 Detailed investigations of communications activity may be undertaken where a specific need has been identified. These processes are explained in the Research Council Acceptable Use Policy for Information and Communication Technology Systems and Services.

5. Security guidance

5.1 Employees should be aware that social media networking websites are a public forum, particularly if the employee is part of a "network". Employees should not assume that their entries on any website will remain private. The content of social media websites could potentially remain online forever and is open to being republished in other media.

5.2 Employees are advised to be security conscious for example by making use of and understanding their online privacy settings. In practice this means being aware of who can see their personal details and generally limiting the amount of personal information that they give out. Reducing the personal information placed on such sites also helps to protect against identity theft.

5.3 In addition, to safeguard the Research Council, when using social networking websites in a personal capacity, employees should:

- ensure that no information is made available that could provide a person with unauthorised access to the establishment/Research Council and/or any confidential work related information
- refrain from recording any confidential information regarding the establishment/Research Council on any social networking website
- always comply with Research Council and local policies, as well as national and international legislation
- .

6. Disciplinary action

6.1 Failure to comply with the Research Council's policy on the Personal Use of Social Media may lead to action in line with the Research Council's disciplinary procedure; misuse of social media could also lead to legal or criminal prosecution.

7. Policy review

This policy will be regularly reviewed to incorporate any legislation changes. The TU may request that a policy is reviewed.

8. Amendment history

Version	Date	Comments/Changes