Computing Regulations 2012

Scope

1. The following Computing Regulations apply to all University staff and students and to any other users of University computing services. They cover the use of all ICT facilities (computer hardware and applications, networks, telephones and related facilities) owned, managed or used by the University; services and equipment provided by ISS, academic and administrative departments; personally-owned hardware using the University’s networks and equipment elsewhere accessed via the University.

Legislation

2. It is the individual user’s responsibility to comply with all applicable UK and European legislation covering the use of ICT facilities. This includes, but is not limited to:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Data Protection Act 1998
- Obscene Publications Acts 1959, 1964
- Protection of Children Act 1987
- Telecommunications (Lawful Business Practices) (Interception of Communications) Regulations 2000
- Telecommunications Act 1984
- Terrorism Act 2006

The Joint Information Systems Committee (JISC) Legal Information Service provides information on the legal obligations of all users of UK HE computing facilities:

http://www.jisclegal.ac.uk/

Acceptable use

3. The primary use and purpose of the University’s computing facilities is to further the University’s mission of research, learning and teaching and the promotion of links with the local community.

4. Users must comply with the following policies:

JANET Acceptable Use Policy
http://www.ja.net/services/publications/policy/aup.html

Eduserv CHEST Use of Software and Datasets
http://www.eduserv.org.uk/chest/appendix-b.html

5. In particular, users must follow the JANET Acceptable Use Policy, which forms part of the University’s Computing Regulations:
JANET may not be used by a user organisation or its members for any of the activities described below:

- Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
- Creation or transmission with the intent to defraud.
- Creation or transmission of defamatory material.
- Creation or transmission of material such that this infringes the copyright of another person.
- Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe.
- Deliberate unauthorised access to networked facilities or services.
- Deliberate activities having, with reasonable likelihood, any of the following characteristics:
  - wasting staff effort or networked resources, including time on end systems accessible via JANET and the effort of staff involved in the support of those systems;
  - corrupting or destroying other users' data;
  - violating the privacy of other users;
  - disrupting the work of other users;
  - denying service to other users (for example, by deliberate or reckless overloading of access links or of switching equipment;
  - continuing to use an item of networking software or hardware after JANET(UK) has requested that use cease because it is causing disruption to the correct functioning of JANET;
  - other misuse of JANET or networked resources, such as the introduction of viruses or other harmful software via JANET.

Where JANET is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of JANET. Any deliberate activity as described in clause 19 above, and where applied to a user of that network, will also be regarded as unacceptable use of JANET.

Use of your account at a JANET Roaming Service (JRS) enabled site is subject to:

- The JANET Acceptable Use Policy
- Any local Acceptable Use and/or other policies

Any breach of industry good practice (as represented by the standards of the London Internet Exchange) that is likely to damage the reputation of the JANET network will also be regarded prima facie as unacceptable use of JANET.

6. Users are not permitted to view, create or transmit material on University or other ICT services which might constitute harassment or bullying under the University's Dignity at Work and Study policy. The viewing, creation or transmission of material in contravention of the University's Equal Opportunities Policy, Race Equality Policy, Sexual Orientation Policy or any other relevant policy is also not permitted.
7. Limited personal use of University ICT facilities is permitted which should normally take place outside of standard working hours. This must conform to the Computing Regulations and should not compromise the user’s study or work obligations to the University. Limited personal use of this sort is subject to the monitoring of use listed under Section 9 below.

Liability

8. Any computing facility provided by the University (including software) is used entirely at the risk of the user. The University will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of any of its computing facilities. Although every effort will be made to maintain services, facilities and the integrity of information and software, the University accepts no responsibility for the malfunction of any computing facilities, the loss of any data or software or the breach of any security mechanisms.

Monitoring of use

9. The University reserves the right to monitor the use of University computing facilities. This monitoring will comply with the Regulation of Investigatory Powers Act 2000 and with the University’s Data Protection Policy and will only take place under the following circumstances:

- Establishing the existence of facts to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought be to be achieved
- In the interests of national security
- Preventing or detecting crime
- Investigating or detecting unauthorised use of telecommunication systems
- Monitoring business-related communications and for deciding whether a communication is business-related
- Ensuring, or as an inherent part of, effective systems operation including compliance with these Regulations.

The Guidelines for the monitoring of computer, telephone and postal communications can be found under regulations.

Code of conduct

10. Users must take all reasonable steps to protect the security of their usernames and passwords. They must not make their usernames and passwords available to anyone else nor use any other user’s username and password.

11. Impersonation of another user to gain access to facilities or to disguise their identity is a serious breach of these Regulations.

12. All users should protect their personal information when using social networking sites. In particular, care should be taken to ensure:

- Protection of privacy
- Protection of identity
- Avoidance of identity theft
To ensure e-safety, all users should follow the Information Commissioner’s Office guidelines at:  


The following guidelines prepared by Information Services at Cardiff University are also recommended:  
[http://www.cardiff.ac.uk/insrv/it/help/safe/protect.html](http://www.cardiff.ac.uk/insrv/it/help/safe/protect.html)

13. The University staff and student e-mail lists are intended for University topics only. All messages sent to the list should show tolerance and respect to all potential recipients. It should be noted that offensive remarks and material could constitute harassment under the University’s Dignity at Work and Study policy. All users of the staff and student e-mail lists should follow the Guidelines at:

**Staff email list guidelines**

14. All students and staff should regularly check their messages on the University e-mail service. Central services and departments will normally use the University e-mail service to communicate with students and staff. Failure to check this service regularly will result in the loss of important academic and financial information.

15. Users must comply with the University’s Information Security Policy. To maintain the integrity of University networks, the Network Connection Policy aspects of the Information Security Policy must be followed, with no connection of any equipment (including wireless devices) to the University’s networks without authorisation. Also, users should not send bulk or unsolicited e-mails to users outside of the University.

16. Users are responsible for any personal data they may hold and must take adequate steps to protect it. Personal data held on laptops, memory sticks and other mobile devices should only be taken off University premises with the permission of the appropriate line manager. Personal data taken away from University premises in this way should be encrypted.

**Sanctions**

17. The University reserves the right to withdraw computing facilities from any user:

- While investigating a breach of these regulations or any other University regulations and disciplinary procedures
- To maintain the operational integrity of computing facilities and services
- As a result of any criminal investigation

18. Any infringement of these Computing Regulations will constitute an offence under the Disciplinary Procedures for students or the University’s terms and conditions of employment for staff. This may result in one or more of the following:

- Suspension by the Director of ISS of the right to use computing facilities
- The imposition of special conditions of use
- University disciplinary proceedings
- Criminal or civil prosecution
In the case of a major breach of Computing Regulations, the Director of ISS shall report such cases to the Pro-Vice-Chancellor (Administration) or in his absence a nominated alternate. However, in the case of an offence which falls under the Disciplinary Procedures, the Director of ISS may report such a breach to the Academic Registrar to be considered under the Disciplinary Procedures.

19. Requests to review the application of any sanctions under the Computing Regulations should initially be raised with the member of ISS staff responsible for that service. If this cannot resolve the problem, then it should be referred to the Director of ISS, or one of the Deputy Directors of ISS. If, exceptionally, this does not resolve the query, then the matter may be referred to the University’s Final Stage Appeals Regulations via the Academic Registrar.

20. Similarly, any complaint about computing services should be raised with the appropriate member of ISS or School staff responsible for that service. If this cannot resolve the problem, then it should be discussed with the Director of ISS, the appropriate Head of School or another appropriate senior member of University staff. If, exceptionally, this does not resolve the problem, then a formal complaint can be made under the University regulations.