Information Services

Regulations for the Use of Information Technology (IT) Facilities at the University of Kent

Scope

1. These regulations apply to
   • All students registered at the University, all members of staff employed by the University, former staff and alumni all visitors and others using the IT facilities provided by the University;
   • All of the University’s IT systems and equipment (whether they are managed by Professional Services or Academic Schools), which includes the University network and all systems directly or indirectly connected to the network; and services provided off-site by third parties contracted to do so by the University;
   • All academic, research, administrative and other users of the University’s IT facilities; and
   • The production of any material using the University’s facilities (as well as personal and University email accounts), including but not limited to printed output, web pages, social networking sites, bulletin boards and news group entries on University MyFolio, forums and blogs.

The Law

2. It is the individual user’s responsibility to comply with all applicable UK legislation, including (but not limited to):
   • The Computer Misuse Act (1990)
   • The Data Protection Act (1998)
   • The Copyright, Designs and Patents Act (1988)
   • The Obscene Publications Acts (1959, 1964)
   • The Telecommunications Act (1984)
   • The Telecommunications (Fraud) Act 1997
   • The Race Relations Act (1976, 2000 Amendment)

3. Users must not use University IT facilities to hold or process personal data except in accordance with the Data Protection Act 1998. Anyone wishing to use the facilities for such a purpose is required to register with the authorised officer in the University Registry. A user must comply with any restrictions imposed concerning the manner in which data may be held or processed and may be held legally responsible for any liability resulting from failure to comply with the provisions of the Act.

4. It is the user’s responsibility to comply with the following documents:
   • The JANET Acceptable Use Policy;
   • The CHEST User Acknowledgement of Third Party Rights
5. It is the user’s responsibility to comply with all advertised special conditions attached to the use of particular services provided by the University.

6. Users are reminded that many aspects of electronic communications are protected by intellectual property rights which are infringed by downloading, uploading, posting, copying, possessing, processing and distributing material from the internet.

**Liability**

7. Any IT facility (including software) provided by the University 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 IT facility. Although it takes reasonable care to prevent the corruption of information, the University does not give any warranty or undertaking to the user about the integrity of information.

8. The University accepts no responsibility for the malfunctioning of any computing hardware, software or facility.

9. The University accepts no responsibility for the loss of any data or software or the failure of any security or privacy mechanism.

10. No claim shall be made against the University, its employees or agents in respect of any loss alleged to have been caused whether by defect in the resources or by act or neglect of the University, its employees or agents.

**Authorised Use**

11. Any student registered with the University, any member of staff, alumni, visitors and all individuals who have been assigned a Kent user account will have signed an undertaking to abide by these Regulations - they are therefore considered to be an authorised user of the University’s IT facilities.

12. All users must notify the University of any change in their status that may affect their right to use IT facilities.

13. All users are responsible for setting their own password and file permissions. It is the user’s responsibility to take reasonable precautions to minimise the risk of unauthorised access by following the University’s advice on ‘changing your IT account password’.

14. Whilst limited personal use of the internet is permitted by staff, all users should be mindful of the following points:

   14.1 When visiting any internet site, information identifying your PC and the network you are connected to may be logged. Therefore any activity you engage in on the internet using a University or personal computer or device connected to the University’s network could affect the reputation of the University.

   14.2 If users choose to use University IT facilities for personal correspondence, they must expect only limited privacy because the University may need to monitor communications for the reasons given in Paragraphs 15 and 16.
14.3 The use of any University IT facility for commercial gain must have the explicit written permission of the Director of Information Services and may be subject to a charge.

14.4 Staff should remind themselves that all email sent and received is deemed to be work related for the purposes of monitoring.

14.5 By making personal use of the University’s facilities to send and receive email you signify your agreement to abide by the conditions imposed for its use, and signify your consent to the University monitoring your personal email in accordance with Paragraph 15 and 16.

Monitoring

15. The University keeps logs of the use of IT systems and services, for example electronic mail and web access. Third-party providers may also maintain activity logs for out-sourced services. These logs are used for purposes connected with the provision and operation of those services and facilities and in the circumstances described in the following paragraph.

16. The University does not routinely monitor individual users’ use of IT facilities and services but, in compliance with the RIP Act 2000, may do so in the following circumstances:

- To establish compliance with UK legislation, these Regulations and other University regulations;
- To investigate or detect unauthorised use of the University’s or other IT facilities;
- To secure effective system operation or as an inherent part of system operation;
- To prevent or detect crime; or
- In the interests of national security.

Behaviour

17. Users must not create, display, produce or circulate any material in any form or medium using their Kent IT account and/or the Kent network:

- That is liable to cause offence, including pornographic material or abusive language;
- That could be described as harassment or bullying as defined by the University’s Dignity at Work Policy
- That could be considered defamatory;
- That breaches copyright;
- That discriminates on the grounds of race, gender, disability, sexual orientation, age, marital status, political or religious belief or contravenes the University’s Equality and Diversity Policy; or
- That damages the reputation of the University.
18. Users of IT facilities must show consideration for others and not interfere with other users.

19. Users are responsible for his/her username and password. They should not knowingly allow anyone to use the username and password under any circumstances.

20. Users must not impersonate another user to gain access to facilities, or disguise his/her identity in an attempt to fake another user.

21. Users must not send or forward junk or chain email and not use email for the mass distribution of unauthorised unsolicited messages.

22. Users must not deliberately introduce a virus nor take any action to circumvent, or reduce the effectiveness of, any anti-virus precautions established by the IT service.

23. Users must not attempt to circumvent access controls placed on the University’s IT facilities and services, or other systems external to the University, or store any software designed to circumvent access controls.

24. Users must not damage any of the University IT facilities or any of the accommodation or services associated with them.

25. Users must comply with the licence agreements of all software and datasets and use the software and datasets only for the purposes defined in these agreements. Users must not load on to the University’s IT facilities any software or datasets contrary to licence agreements or any software that interferes with the normal working of the equipment.

26. Users are required to respect the copyright of all materials, software and datasets made available by the IT service and third parties.

27. Users must not delete or amend the data of any other user without their prior permission.

28. Users must not connect any equipment to the University’s network without prior authorisation and any connection of equipment to the University’s network must be done in accordance with the University’s Information Technology Security Policy.

Withdrawal of Access Rights

29. The University reserves the right to withdraw users’ access rights to IT services and facilities in the following circumstances:

- While investigating a suspected breach of these or other regulations;
- As part of the published disciplinary procedures;
- In order to maintain the operational integrity of the IT systems provided; or
- At the reasonable request of a Principal Officer of the University.

Infringement
30. The University will investigate any suspected breach of these Regulations according to the procedures described in the document Computer Misuse Procedure for Students, Staff, Alumni and External Users.

31. Infringement of these Regulations may constitute a disciplinary offence under the University's Regulations on Student Discipline in relation to non-academic matters, in the case of a student, and the University's Terms and Conditions of Employment, namely the Disciplinary and Dismissals Procedure Agreement for Staff in Grades 1-6 or the Code of Practice under Statute 7 in the case of a member of staff.

32. Any evidence that a criminal act has been committed will be passed to a Principal Officer of the University and may be reported to the police.

Approved 23 March 2012