IT Acceptable Use Policy 2016-2017

1 SCOPE

These regulations apply to:

1.1 All users of services provided by, or for which access is facilitated by, the University.

1.2 Any equipment owned by the University, or equipment for which access has been facilitated by the University.

1.3 Use of systems and services owned by other bodies, access to which has been provided by the University. In such cases, the regulations of both bodies apply. In the event of a conflict of the regulations, the more restrictive takes precedence.

2 APPLICABLE LAWS AND POLICIES

Those who use the facilities in the UK are bound by the laws of the UK, and other policies of the University. A list is given in Appendix A.

3 INFRINGEMENT

Staff or students infringing these regulations may be liable to disciplinary action. These regulations apply subject to and in addition to the law. Any infringement of these regulations may also be subject to penalties under civil or criminal law and such law may be invoked by the University. Use of the University's systems may be logged to permit the detection and investigation of infringement of Policies.

4 USE

4.1 Before using any IT facilities, users must be authorised by completing the registration process.

4.2 The University's IT facilities must be used for the purposes and in the way they were intended to be used. Other use may be allowed as a privilege, not a right.

4.3 Use of the University's IT facilities must not bring the University into disrepute.

4.4 Users must not cause damage to the University's IT facilities, nor to any of the accommodation or services associated with them.

4.5 Users must adhere to the terms and conditions of all licence agreements relating to IT facilities and information which they use including software, data, equipment, services, documentation and other goods.

4.6 Users must not infringe copyright works in any form including software, data, documents, images, or audio or video recordings.

4.7 Users must not load any software onto the IT facilities without permission from IT Services

4.8 Users must take all reasonable precautions to ensure that they do not deliberately or recklessly introduce any virus, worm, Trojan, malware, or other harmful or nuisance program or file into any IT facility. They must not take deliberate action to circumvent any precautions taken or prescribed by the University to prevent this. They must take all reasonable precautions to avoid infection, by, for example, not opening email attachments of unknown source.

4.9 Users must not access, delete, amend or disclose the data or data structures of other users without their permission.

4.10 Users must not act in any way which puts the security of the IT facilities at risk. In particular, user credentials must be kept safe and secure and only used by those authorised to do so.

4.11 Users must not in their use of IT facilities exceed the terms of their registration. In particular they must not connect to or attempt to connect to any computing IT facility without the permission of IT Services. This is known as hacking and is a criminal offence in terms of the Computer Misuse Act 1990, as amended.

4.12 Users may be liable for the cost of remedying any damage they cause.

4.13 The use of IT facilities or information for commercial gain must have the explicit prior permission of IT Services and may be subject to charge.

4.14 The use of IT facilities or information to the substantial advantage of other bodies, such as employers of placement students, must have the explicit prior permission of IT Services and may be subject to charge.

4.15 Except by prior arrangement users should not carry out activities that will significantly interfere with the work of other users.

4.16 Users must not attempt to conceal or falsify the authorship of any electronic communication.

4.17 Users must not send unsolicited electronic communications to multiple recipients except where it is a communication authorised by University. Specifically, users must not use the University's facilities to send spam or chain letters. If in doubt, advice must be sought from IT Services.

4.18 The creation, display, production or circulation of material which is illegal, likely to cause offence or which promotes terrorism is forbidden. Where access to such material is deemed necessary, permission must be sought from IT Services.

4.19 Any infringement of these regulations constitutes a disciplinary offence under the applicable procedure and may be treated as such regardless of legal action. Sanctions can range proportionally from withdrawal or suspension of IT facilities to, or more serious breaches, expulsion for students or dismissal for staff where Gross Misconduct is established.

5 DISCLAIMER

The University makes no representations about the suitability of this service for any purpose. All warranties, terms and conditions with regard to this service, including all warranties, terms and conditions, implied by statute, or otherwise, of satisfactory quality, fitness for a particular purpose, and non-infringement are excluded to the fullest extent permitted by law.

The University shall not in any event be liable for any damages, costs or losses (including without limitation direct, indirect, consequential or otherwise) arising out of, or in any way connected with, the use of the service, or with any delayed access to, or inability to use the service and whether arising in tort, contract, negligence, under statute or otherwise. Nothing in these terms excludes or limits liability for death or personal injury caused by the negligence of University in providing this service.

Appendix A.

1 LAW

Applicable laws and policies include the following together with any amendments and any superseding legislation which may be enacted.

a. Obscene Publication Act 1959 & 1964
b. Protection of Children Act 1978
c. Police and Criminal Evidence Act 1984
d. Copyright, Designs & Patents Act 1988
e. Computer Misuse Act 1990
f. Human Rights Act 1998
g. Data Protection Act 1998
h. Regulation of Investigatory Powers Act 2000
i. Freedom of Information Act 2000
j. Employment Code of Practice 2002
k. Prevention of Terrorism Act 2005
l. Terrorism Act 2006
m. Police and Justice Act 2006

Applicable policies include:

a. JANET Acceptable Use Policy
b. RAU Information Security Policy and Procedures
c. RAU Data Protection Policy
d. RAU Privacy Policy
e. RAU PCI-DSS Policy
f. RAU Freedom of Information
g. RAU RIPA Policy
h. RAU Copyright Policy
i. RAU Email Policy
j. RAU Social Networking Policy
k. RAU Mobile Computing Policy
l. RAU Residential Network Policy
m. Other relevant policies

This list is not exhaustive and will be subject to change.

Contact us

For any queries concerning this policy please contact Head of IT