Wireless service policy

1. **eduroam policies:** When using the eduroam service, you must also obey the JANET eduroam policy and any policies of organisation providing the eduroam access.

2. **Acceptance of responsibility:** A user will be held responsible for any breach of regulations carried out using a connection authenticated with their username. This includes action taken by others.

3. **Identification:** You must not attempt to authenticate yourself using another person's or organisation's credentials.

4. **Network security:** The Centre reserves the right to conduct scans of the network in order to determine what computers are connected to it and what services they are operating. You must not configure your computer to use any network address other than those allocated to you.

5. **Computer security:** Wireless service users must take all practical steps to make sure that equipment connected to the wireless service is virus free and adequately secure. All users must have anti-virus protection installed (as appropriate for the device platform) and that any installed anti-virus software protection is kept up-to-date. Users should also run a local personal firewall (Windows, Mac and Linux built-in firewalls are acceptable) and keep operating system security patches up-to-date. Failure to comply with this can result in your wireless equipment being disconnected from the wireless service whilst the problem is resolved, for which responsibility lies with the device owner

6. **Service operation:** You must not do anything that interferes with the operation of the wireless service. This includes running web/file servers and illegal file sharing or peer-to-peer software, these can use excessive bandwidth and/or assist in the distribution of illegal or copyright data, software, music, video/movies or images.
   It is also prohibited to use or connect equipment of any kind which can be classed as insecure or create interference, especially to the University wireless service. Any such prohibited services or devices discovered shall lead to the permanent termination of the wireless service.
7. **Copyright:** It is illegal and against Centre regulations to copy or share movies, music, software and other copyrighted material without permission from the copyright holder. You must not do this, whether intentionally or as a failure to correctly configure a file sharing program on your computer.

8. It is prohibited to use the wireless service to attempt unauthorised access to another computer or network devices (on or off site).

9. **Legislation:** The Centre has an obligation to abide by all UK legislation and relevant legislation of the EC. The requirement for compliance devolves to all users defined above, who may be held personally responsible for any breach of the legislation. Further details on how the legislation relates to the work of the Centre is available from the IT Department. Of particular importance in the respect of the Centre are:

- Computer Misuse – The Computer Misuse Act (1990)
- Copyright – The Copyright, Designs and Patents Act (1988)
- Data Protection – The Data Protection Act (1998)
- Offensive or defamatory material – The Defamation Act (1996), the Obscene Publications Act (1959), the Protection of Children Act (1978) and the Criminal Justice Act (1988)
- Discrimination – The Sex Discrimination Act 1975, the Race Relations Act (1976) and the Disability Discrimination Act (1995), the Employment Equality (Sexual Orientation) Regulations 2003 and the Employment Equality (Religion or Belief) Regulations 2003

10. **Sanctions:** If a user is in breach of this policy the IT Department may, withdraw or restrict his or her use of computing facilities and user account. Any breach of the regulations may be reported to the Warden to be dealt with under the Centre's disciplinary procedures. Where appropriate, breaches of the law will be reported to the relevant authorities.