hallsnet neuaddrwyd IT Rules and Regulations

1. Introduction

1.1 These rules and regulations apply to the Cardiff Metropolitan University Halls of Residence network (HallsNet) and must be adhered to by all users of that network.

1.2 HallsNet utilises JANET for Internet connectivity and may therefore only be used by registered students, members of staff and guests who are visiting for academic and/or research reasons.

1.3 Breaches of these Rules and Regulations may be dealt with under the relevant disciplinary procedure and may, where an offence has occurred under any current law or regulation, be reported to the police, or other appropriate authority.

2. Conditions of Use

2.1 Cardiff Metropolitan University reserves the right to monitor the use of this network where it believes that these regulations or other applicable law may have been breached.

2.2 HallsNet is provided solely for the use of the residents of these halls and its use in furtherance of business gains or for commercial purposes is prohibited.

2.3 Use of the HallsNet services is granted by allocation of a User Name. Users must not use another person's User Name, nor allow any password issued to them to become known to any other person.

2.4 Cardiff Metropolitan 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 this 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 Cardiff Metropolitan University in providing the service.

3. Regulations

3.1 General

3.1.1 Any use of this service is bound by the laws and legislation of the UK.

3.1.2 Usage of Cardiff Metropolitan University's IT Services (Blackboard, Locate, Outlook Live, etc) must be done in compliance with the Electronic Communications Policy.

3.1.3 Any PC, MAC and Laptop equipment that are connected must have up-to-date security patching and Anti-Virus, Anti-Spyware and Personal Firewall software installed.

3.1.4 It is the responsibility of each study bedroom's occupant to ensure that any usage of the wired network point in their room is done so in compliance with these rules and regulations.

3.1.5 Users are not permitted to provide any kind of network service, such as Internet Connection Sharing, DHCP or DNS Servers or Web Services. In addition the attachment of network equipment or devices, such as routers, switches, wireless access points or multi-homed computers, is also prohibited.

3.1.6 The use of static IP addresses is not permitted and any equipment connected must be set to use DHCP.

3.2 Unacceptable Use

Any usage for the purposes listed below or any other use which may bring Cardiff Metropolitan University into disrepute are a breach of these regulations.

a) The creation, transmission, publication, viewing, posting or distribution of any material or comments which are obscene, pornographic, racist, vulgar, discriminatory, defamatory, fraudulent, aggressive, otherwise illegal or that is likely to create any liability or cause harassment, annoyance, inconvenience or needless anxiety.

b) The unauthorised transmission of unsolicited commercial or advertising material and in addition the creation or forwarding of chain emails, pyramid schemes or nuisance emails. It is also prohibited to attempt to conceal or falsify the authorship of an email or any other form of electronic communication.

c) Gaining or attempting to gain unauthorised access, misuse of confidential information, packet-sniffing, port-scanning, corrupting or destroying data, violating privacy, disrupting the work of others or carrying out activities which deliberately denies, restricts or reduces service. This includes IT systems and resources that are internal to Cardiff Metropolitan University and also external systems on Internet.

d) Any deliberate activities which lead to disruption of communication services, wasting support staff effort, IT resources or network bandwidth.

e) The use of Peer-to-peer software for file-sharing applications or the transmission of content that breaches a third party's copyright or patent or deliberately discloses their confidential information.