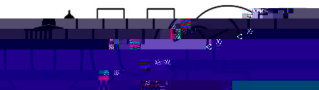# Information Security Policy
University College London

UCL depends heavily upon its IT network for research, teaching and administrative activities. It is essential that the stability, integrity and security of the UCL IT network be safeguarded for use by all members of UCL. To help ensure an effective, highly available network and to facilitate the rapid tracking down and resolution of any problems, UCL's Information Risk Governance Committee has agreed the following policy.

The scope of the policy covers all equipment irrespective of ownership that is attached to network data points on the UCL network or uses UCL provided Wireless Access. For the avoidance of doubt, this includes Student Halls of Residence. For the purposes of clarification, this includes, but is not limited to, desktop computers, laptops, servers, printers, mobile phones, reprographic and audio visual devices. The target audience comprises end users, network managers and IT system administrators.

'Attachment' is defined as any method of connection to the UCL Campus network that results in the device being allocated an IP address belonging to or managed by UCL. This

2.3   All requests for network connections should be directed to the relevant Departmental Network Administrator.

2.4   The Departmental Network Administrator will allocate IP addresses to individual machines from subnets delegated to them.

IP addresses may not be moved from one machine to another without the permission of the Departmental Network Administrator; except where a department elects to use a dynamic allocation scheme (e.g. DHCP).

2.5   The Departmental Network Administrator will ensure that all IP addresses in use are registered with an appropriate entry in the Domain Name System.

Guidance on naming schemes is available from ISD

2.6   The Departmental Network Administrator must ensure that any required network details e.g. broadcast address, network masks, and gateway addresses, are correctly provided

2.7   The Departmental Network Administrator must ensure that sufficient records are kept for each device connected to the LAN so that systems, their location and their custodian can be readily identified should problems arise.

2.8   DHCP logs should be retained in line with UCL's retention schedule.

Where DHCP is employed, logs must include IP address allocation, so that it is possible to determine what system had use of a particular address at a given time.

2.9   Departmental Network Administrators must keep records of the physical and topological organization of LANs under their control.

2.10   Departments must disconnect system(s) from the network when requested to do so by the Information Security Group or ISD Network Services. Such requests would typically follow a system causing problems to other users of the UCL network or to an external network and/or following a major security breach. Systems must not be reconnected to the network without the explicit authorisation of the Information Security Group

2.11.   Requirements for wireless connections are laid out in Section 4

2.12   Use of private address spaces (RFC 1918) must comply with the policy laid down by the ISD Network Services Group

3   ISD Information Systems responsibilities

3.1.   ISD allocates network address blocks to Departmental Network Administrators as needed. Departments are normally free to determine how allocated addresses within these blocks are used

3.2   ISD advises UCL on appropriate higher-level naming schemes for networked systems. Departments must abide by these conventions.
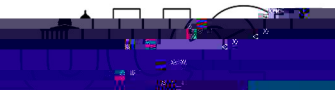
3.3 The protocols currently approved by UCL for use over the UCL backbone network
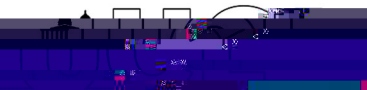
Users must not turn their device into an access point or an ad hoc network unless all devices on the ad hoc network are isolated from the UCL Network

4.5 ISD Network Services must approve the frequency/channel usage, power output and the antenna profile of all wireless access points. The approved frequency/channel usage may be subject to change as usage grows. This may necessitate existing installations to be modified. APs that cause interference must be remedied or removed. This includes Wireless Access Points used for research purposes.

4.6 All non conforming equipment must be remedied or removed on request of the Information Security Group.

5 Institutional Firewall

5.1.