
UCL Policy on connecting equipment to the college network

Information Security Policy
University College London

Document Summary

| | |
|-----------------------------------|---|
| Document ID | TBD |
| Status | Approved |
| Information Classification | Public |
| Document Version | Endorsed by the Information Strategy Committee, 27 November 2008 |

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 Strategy 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. For the purposes of clarification, this includes, but is not limited to, desktop computers, laptops, servers, printers, personal digital assistants, reprographic and audio-visual devices. The target audience comprises end-users, network managers and IT system administrators.

'Attachment' is here taken to include any mechanism which allows equipment to access UCL network resources without the involvement of external service providers. Thus attachments made to the UCL network using wireless networking technologies, for example, are subject to this policy, whilst connections via modems routed through an ISP are not, even if the destination is an official UCL service.

1. User Responsibilities

- 1.1. All users of the network must be aware of and abide by the UCL Computing Regulations and the JANET Acceptable Use Policy as operated by JANET(UK).
- 1.2. New connections of equipment to departmental networks attached to the UCL backbone network may be made only with the authority of the department's Departmental Network Administrator (see 2.2).
- 1.3. Students in halls of residence may connect computing equipment to the network data points in study bedrooms only after registering their connection with ISD Information Systems. Such systems are then subject to all statutory and UCL rules and regulations currently in force.
- 1.4. Access points (e.g. leased lines to ISPs or modems supporting dial-in) may be introduced into departmental networks only with the permission of the Head of Department. In addition, the ISD Information Systems Network Group must be notified. Additional requirements apply to all wireless connections (see Section 4).
- 1.5. Connections between the UCL production and research networks (including the dual homing of systems) must not be made except by prior arrangement with IS Network Group and CST on appropriate security policies and their method of implementation.
- 1.6. Custodians should ensure that login-names and passwords are issued only to registered users. Registration should as a minimum obtain user contact details and written confirmation that they have seen and agree to abide by the UCL Computing Regulations. Accounts should be issued only for bona fide purposes in pursuance of UCL business.

Access must be restricted to authorized users and those users must be required to login formally with a secure login-name/password combination.

- 1.7. Connected equipment must be maintained in accordance with manufacturers' recommendations. In particular, operating system and application software should be kept up-to-date to ensure that security vulnerabilities are not created. Equipment must not be, or remain, connected to the network after a manufacturer ceases to provide security patches, without the prior approval of the Computer Security Team.
- 1.8. All equipment connected to Local Area Networks (LANs) must conform to the appropriate IEEE specifications. Only those protocols supported by UCL may be run across the backbone (see 3.3).

If doubt exists, the ISD Service Desk should be contacted before the equipment is connected (email servicedesk@ucl.ac.uk, telephone 020 7679 5000 / extension 25000 within UCL).

2. Departmental/Divisional Responsibilities

- 2.1. Each head of department shall ensure adequate oversight of security (in consultation with the UCL Computer Security Team) either through departmental computing support staff or equivalent.
- 2.2. Each head of department should establish a named Departmental Network Administrator, who will be responsible for overseeing the operation of the LAN either in person or by delegating duties to other named individuals.

The duties and training requirements of Departmental Network Administrators are set out in a code of practice associated with the information security policy.

- 2.3. All requests for network connection should be directed to the relevant Departmental Network Administrator.
- 2.4. The Departmental Network Administrator will allocate IP addresses to individual machines.

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 Information Systems.

- 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 for six months.

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 written records of any physical re-organisation of their LANs.

2.10. Departments must disconnect system(s) from the network when requested to do so by CST or IS Networks. 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 CST.

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

3. ISD Information Systems responsibilities

3.1. ISD Information Systems 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 Information Systems 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 are those comprising the TCP/IP protocol suite.

Although a small number of existing systems continue to depend on legacy protocols, any newly commissioned systems must make use only of the approved protocols.

3.4. Physical connections to the UCL backbone network may be made only by ISD Information Systems.

3.5. ISD Information Systems may, on behalf of UCL, and subject to appropriate consultations, restrict excessive use of the backbone bandwidth.

3.6. In the event of unacceptable network events occurring on a LAN or in order to safeguard the security of other systems, ISD Information Systems has the right to gain access to and inspect the configuration of devices or equipment on that network and to require the immediate removal of any devices or equipment that it believes could be the source of the problem.

3.7. In the event of unacceptable events on a LAN causing problems on another part of the College network or on an external network, or in order to safeguard the

security of other systems, ISD Information Systems has the right to disable any or all of the LAN, as necessary, in order to remove the source of the problem.

While every effort will be made to contact the Departmental Network Administrator, Head of Department and/or other appropriate persons, this may not always be possible. All services will be reconnected at the first opportunity once the underlying problem has been resolved.

- 3.8. Failure to comply with this policy may result in immediate disconnection from the network.

4. Wireless

- 4.1. All wireless access to the UCL LAN must be authenticated and logged.
- 4.2. Departments requiring new wireless connectivity should normally make use of RoamNet as it offers a secure solution and should meet most requirements. Where exceptional cases arise, departments may be permitted to have separate arrangements which would provide the required access. These must provide at least the level of security of the RoamNet service.
- 4.3. ALL methods of wireless connection to the UCL LAN must be approved by the Computer Security Team. CST will assess if authentication, encryption, security and logging mechanisms are adequate using "Guidelines 4 – Operational Criteria for Wireless Access Installations).
- 4.4. ALL wireless access points must be registered with CST. This includes access points which do not connect to the UCL network.
- 4.5. IS Networks 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 which cause interference must be remedied or removed.
- 4.6. All non-conforming equipment must be remedied or removed on request of CST.

5. Institutional Firewall

- 5.1. A policy of 'default deny inbound' and 'default permit outbound' will apply. Servers which are intended to be accessible from outside UCL will need to be registered and approved by the Computer Security Team.
- 5.2. All parts of UCL (i.e. all of the UCL IP address space) will be protected by the Institutional Firewall.
- 5.3. Exemptions from section 5.2 may be permitted for IP addresses used entirely for research into networking provided this is by prior agreement with IS Network Group and the Computer Security Team. All routing between such addresses and other parts of the UCL internal network must be via the Institutional Firewall.

6. Avoidance of clear text passwords

Transmission of passwords across the network as clear text represents a major security risk.

New applications and systems must transmit and/or accept passwords or other authorization credentials only if strongly encrypted. Existing uses of clear-text authentication should be disabled as rapidly as practicable; if encrypted procedures are not supported, the Computer Security Team must be contacted for advice.

7. Monitoring of computer and network use

Any monitoring of systems or networks may be carried out only in accordance with the UCL Policy on Monitoring Computer and Network Use.

8. Status of this document

This document is a part of UCL's information security policy and has been approved by UCL's Information Strategy Committee.

9. References

UCL Computing Regulations:

<http://www.ucl.ac.uk/cert/swg/policy/Regulations.html>

JANET Acceptable Use Policy:

<http://www.ja.net/services/publications/policy/aup.html>

Information on halls of residence connections:

<http://www.ucl.ac.uk/is/halls/>

UCL Privacy Page (including information on monitoring):

<http://www.ucl.ac.uk/privacy>