LONDON'S GLOBAL UNIVERSITY

UCL Policy on connecting equipment to the UCL network

Information Security Policy

University College London

Document Summary

Document ID	TBD
Status	Approved
Information Classification	Public
Document Version	Approved by the Information Risk Governance Group 10 April 2017

University College London, Gower Street, London WC1E 6BT
Tel: +44 (0)20 7679 2000
www.ucl.ac.uk

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 Group 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, personal digital assistants, 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 therefore includes devices connected using a Virtual Private Network circuit terminating within UCL (e.g. the UCL VPN service) or using a UCL Wireless network. It excludes devices connected to other network providers such as 3/4G mobile networks or WiFi hotspots in Airports or Coffee shops.*

1. User Responsibilities

1.1. All users of the network must be aware of and abide by the UCL Computing Regulations and the Jisc Acceptable Use Policy as operated by Jisc. The full text of their policy can be found at: https://community.jisc.ac.uk/library/acceptable-use-policy.

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. [Left intentionally blank in this revision]

1.4. External connections (including but not limited to leased lines to ISPs, ADSL connections or modems supporting dial-in) may be connected to departmental networks only with the permission of the Head of Department (or delegated authority such as IT Manager) *and* by prior arrangement with ISD Network Services and Information Security Group (ISG). 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 ISD Network Services and Information Security Group (ISG).

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. Systems must run up-to-date anti-malware software where available.

Equipment must not be, or remain, connected to the network after a manufacturer ceases to provide security patches, without the prior approval of the Information Security Group.

1.8. All equipment connected to Local Area Networks (LANs) must conform to the appropriate IEEE specifications for networks. 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).*

1.9. Users must not attempt to circumvent any firewall or software designed to protect systems against harm.

1.10. Unauthorised use of IP addresses or changing of a System MAC address is prohibited. The Departmental Network Administrator or ISD should be approached to obtain an IP address and changing a physical system MAC address should never occur. When assigning a MAC address for a Virtual Machine, the address chosen should have the locally assigned bit set and should be randomly generated. MAC addresses should not be manually assigned. If there is a valid requirement to set a MAC address manually, it must be discussed with the Information Security Group first.

2. Departmental/Divisional Responsibilities

2.1. Each head of department shall ensure adequate oversight of information security (in consultation with the UCL Information Security Group) 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 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 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 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 are those comprising the TCP/IP protocol suite.

3.4. Only ISD Network Services staff are permitted to make changes to the UCL Core network. This includes adding any physical connections..

3.5. ISD Network Services may, on behalf of UCL, and subject to appropriate consultations, restrict excessive use of the Core Network bandwidth. If a user has a requirement for high bandwidth, they should consult ISD Network Services to discuss their requirements.

3.6. In the event of unacceptable network events occurring on a LAN or in order to safeguard the security of other systems, ISD 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 UCL network or on an external network, or in order to safeguard the security of other systems or to protect the reputation of UCL, ISD 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 connections to the UCL LAN must be individually authenticated, logged, and be trackable back to the user.

4.2. Departments requiring wireless connectivity should normally make use of eduroam 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 eduroam service.

4.3. ALL methods of wireless connection to the UCL LAN must be approved by the Information Security Group. The Information Security Group 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 which connect to the UCL network must be registered with ISD Network Services.

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. 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 Information Security Group.

5.2. All parts of the UCL Network (i.e. all of the IP address space managed by UCL) will be protected by a centrally managed UCL Firewall.

5.3. Exemptions from section 5.2 may be permitted for IP addresses used entirely for research purposes provided this is by prior agreement with ISD Network Services and the Information Security Group. 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 encryption is not supported, the Information Security Group 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 Risk Governance Group.

9. References

UCL Computing Regulations:
https://www.ucl.ac.uk/informationsecurity/policy/public-policy/Regulations

JANET Acceptable Use Policy:
https://community.jisc.ac.uk/library/acceptable-use-policy

Information on halls of residence connections:
http://www.ucl.ac.uk/isd/services/get-connected/halls

UCL Privacy Page (including information on monitoring):
http://www.ucl.ac.uk/privacy

Network Policy on use of (rfc 1918) private address space
https://www.ucl.ac.uk/isd/services/get-connected/wired/privateaddress

Wireless access point registration form
http://www.ucl.ac.uk/is/network/wireless/departmental/registration.php

Document Control Sheet
Revision History

Date of this revision: 14.02.2017

Date of next revision: TBD

Revision date	Summary of Changes
14.02.2017	***Replaced*** "college" ***with*** UCL in the title and footer ***Replaced*** all occurrences of "*Computer Security Team*" with "*Information Security Group*" ***Replaced*** all occurrences of "*CST*" with "*ISG*" ***Replaced*** "*IS Network Group*" with "*ISD Network Services*" ***Replaced*** "*Information Systems*" with "I*SD*" ***Replaced*** "*RoamNet"* with "*eduroam*"
	Paragraph 1 ***Replaced "****Information Strategy Committee*" ***with*** "*Information Risk Governance Group*"
	Paragraph 2 ***Added "****or uses UCL provided Wireless Access. For the avoidance of doubt, this includes Student Halls of Residence.****" to*** *"…UCL Network****"*** ***Added*** "*mobile phones,"* ***to*** *"…personal digital assistants, reprographic…"*
	Paragraph 3 ***Deleted*** *"'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."* ***Added*** *"'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."* ***Deleted*** *"This therefore includes devices connected using the UCL VPN or using UCL Wireless networks."* ***Added*** *"This therefore includes devices connected using a Virtual Private Network circuit terminating within UCL (e.g. the UCL VPN service) or using a UCL Wireless network. It excludes devices connected to other network providers such as 3/4G mobile networks or WiFi hotspots in Airports or Coffee shops."*
	1. User Responsibilities ***Replaced*** *"JANET"* ***with*** *"Jisc"* ***Added*** "*The full text of their policy can be found at: https://community.jisc.ac.uk/library/acceptable-use-policy*"

	Deleted "*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 the Information Services Division(ISD) Information Systems. Such systems are then subject to all statutory and UCL rules and regulations currently in force.*" ***Updated*** "*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*." ***with*** "*1.4 External connections Access points (including but not limited to leased lines to ISPs, ADSL connections or modems supporting dial-in) may be connected to departmental networks only with the permission of the Head of Department (or delegated authority such as IT Manager) and by prior arrangement with ISD Network Services and Information Security Group (ISG).*" (1.5) ***Deleted*** "*on appropriate security policies and their method of implementation.*" (1.7) ***Added*** *"Systems must run up-to-date anti-malware software where available."* *(1.8)* ***Added*** *"for networks."* ***to*** *"…IEEE specifications*" ***Added*** "*1.9 Users must not attempt to circumvent any firewall or software designed to protect systems against harm.*" ***Added*** *"1.10 Unauthorised use of IP addresses or changing of a System MAC address is prohibited. The Departmental Network Administrator or ISD should be approached to obtain an IP address and changing a physical system MAC address should never occur. When assigning a MAC address for a Virtual Machine, the address chosen should have the locally assigned bit set and should be randomly generated. MAC addresses should not be manually assigned. If there is a valid requirement to set a MAC address manually, it must be discussed with the Information Security Group first.*"
	2. Departmental/Divisional Responsibilities (2.1) ***Added*** *"information"* **to "***..oversight of security …"* (2.4) ***Added*** *"from subnets delegated to them."* ***to*** "*The Departmental Network Administrator will allocate IP addresses to individual machines.*" (2.9) ***Replaced*** "*Departmental Network Administrators must keep written records of any physical re-organisation of their LANs.*" ***with*** "*Departmental Network Administrators must keep records of the physical and topological organization of LANs under their control.*" ***Added*** "*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 *(3.3)* ***Deleted*** *"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)* ***Replaced*** *"Physical connections to the UCL backbone network may be made only by ISD Information Systems."* ***with*** *"Only ISD Network Services staff are permitted to make changes to the UCL Core network. This includes adding any physical connections*." *(3.5)* ***Replaced*** *"backbone*" ***with*** "*Core Network*." ***Added*** "*If a user has a requirement for high bandwidth, they should consult ISD Network Services to discuss their requirements."* *(3.7)* ***Inserted*** *"or to protect the reputation of UCL"* ***in*** *"…of other systems, ISD has the…"*
	4. Wireless (4.1) ***Replaced*** "*All wireless access to the UCL LAN must be authenticated and logged.*" ***with*** "*All wireless connections to the UCL LAN must be individually authenticated, logged, and be trackable back to the user.*" (4.2) ***Deleted*** "*new*" (4.4) ***Replaced*** "*ALL wireless access points must be registered with CST. This includes access points which do not connect to the UCL network*" ***with*** "*ALL wireless access points which connect to the UCL network must be registered with ISD Network Services.* *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)* ***Added*** *"This includes Wireless Access Points used for research purposes."*
	5. Institutional Firewall (5.2) ***Replaced*** "*All parts of UCL (i.e. all of the UCL IP address space) will be protected by the Institutional Firewall.*" ***with*** "*All parts of the UCL Network (i.e. all of the IP address space managed by UCL) will be protected by a centrally managed UCL Firewall.*" (5.3) ***Replaced*** "*into networking*" ***with*** "*purposes*"
	6. Avoidance of clear text passwords ***Replaced*** "*encrypted procedures are"* ***with*** "*encryption is*"
	8. Status of this document ***Replaced*** "*Information Strategy Committee*" ***with*** "*Information Risk Governance Group*"
	9. References ***Updated relevant weblinks***

Approvals

Endorsed by the Information Strategy Committee	**27-Nov-2008**
Endorsed by the Security Working Group	**22-Feb-2017**
Endorsed by the Information Risk Management Group	**30-Mar-2017**
Approved by the Information Risk Governance Group	**10-Apr-2017**