LONDON'S GLOBAL UNIVERSITY

UCL Policy on Electronic Mail (EMAIL)

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

1. Introduction

Electronic mail (email) is an important means of communication for UCL and it provides an efficient method of conducting much of UCL's business. This document sets out UCL's policy on the use of email, including use for teaching, research and administration.

2. Scope

This policy has the scope defined in section 1.4 of the UCL Information Security Policy and includes, but is not limited to, any UCL system providing email services or any email service accessed from a UCL facility or any email service provided on behalf of UCL or a UCL department by a third party.

The policy affects both users and managers of all such email services.

3. Appropriate Use of UCL Email Services

3.1. Use of email services is subject to all the same laws, policies, and codes of practice that apply to the use of other means of communications, such as telephones and paper records, and shall comply with the UCL Computing Regulations.

All students of UCL and those staff whose duties require it, should have a UCL-provided email account which is to be used for email communications carried out for UCL related activities.

3.2. Users may not use UCL email services and/or facilities, to transmit:

- commercial material unrelated to the legitimate educational business of UCL, including the transmission of bulk email advertising (spamming);
- bulk non-commercial email which is likely to cause offence or inconvenience to those receiving it. This includes the use of email exploders (i.e. listservers) at UCL and elsewhere, where the email sent is unrelated to the stated purpose for which the relevant email exploder is to be used (spamming);
- unsolicited email messages requesting other users, at UCL or elsewhere, to continue forwarding such email messages to others, where those email messages have no educational or informational purpose (electronic chain letters);
- email messages which purport to come from an individual other than the user actually sending the message, or with forged addresses (spoofing);
- material which is offensive or inappropriate;
- material that incites criminal activity, or which may otherwise damage UCL's research, teaching, and commercial activities, in the UK or abroad;
- material to which a third party holds an intellectual property right, without the express written permission of the rightholder;

- material that is defamatory, libellous, harassing, threatening, discriminatory or illegal (see the Guide to Non-discriminatory Language on the Human Resources Division web-site);
- material that could be used in order to breach computer security, or to facilitate unauthorized entry into computer systems;
- material that is likely to prejudice or seriously to impede the course of justice in UK criminal or civil proceedings;
- messages that could imply the creation of an order or contract contrary to UCL Financial Regulations.

3.3. Caution should be exercised when drafting email which references personal data. Encryption may be used to ensure confidentiality, but if there is any uncertainty about such email, advice should be sought from the Data Protection Officer.

3.4. Whilst UCL provides staff with access to email systems for the conduct of UCL-related business, incidental and occasional personal use of email is permitted so long as such use does not disrupt or distract the individual from the conduct of UCL business (i.e. due to volume, frequency or time expended) or restrict the use of those systems for other legitimate users. (See definition of reasonable personal use in the UCL Computing Regulations.)

3.5. Users must not knowingly allow anyone else to send email using their accounts. Users will be deemed liable for any email or activity from their accounts.

3.6. The Information Security Group (ISG) may use email to test user susceptibility and to improve security awareness.

4. Email Servers

Email servers must be registered with ISD in order to be able to send outgoing external email or receive incoming external email. Such servers must not act as open relays nor may they run open proxies.

5. Viruses and other malware

All reasonable steps must be taken to prevent the propagation of computer viruses or other malware by email. Incoming and outgoing email must be routed via mail servers (including any such services operated by third parties on behalf of UCL) which must run adequate malware detection software. Systems must run up-to-date anti-malware software where available; the operating system must also be patched regularly

6. Penalties for Improper Use of Email Services

Failure to comply with this email policy could result in access to the service being withdrawn or, in more serious cases, to disciplinary action being taken, and/or civil action, and/or criminal prosecution. In determining whether email messages are in breach of this policy managers may seek advice from the Director of ISD.

7. Privacy and Security

7.1. Email, like all methods of communication, cannot be assumed to be secure. It cannot be assumed that email will be correctly delivered or that the sender is as claimed in the mail headers. Steps must be taken to minimise the risk of interception or breaches of confidentiality. These steps include:

- not divulging your user passwords to anyone (including in email)
- not knowingly allowing anyone else to send email from your account

You should also consider the following guidelines when sending email:

- ensuring that you identify and use the correct recipient email address
- considering anonymising references to specific individuals
- confirming the identity of an email sender where there is reason to question this
- adopting a risk-based approach to deciding what information is appropriate to be sent by email.

Where an issue is particularly sensitive or confidential, email is unlikely to be a sufficiently secure method of communication and should be avoided.

7.2. The use of email disclaimers is discouraged.

7.3. Users should be aware that deletion of an email message by both sender and receiver does not mean that the message no longer exists on their systems or on the systems through which it passed. Conversely, when a message has been transmitted, it is not necessarily the case that a record of it will exist or be accessible.

7.4. Ex.-staff email will be deleted one year after they leave UCL unless otherwise authorised. For further advice see the UCL Records Management retention schedule available here: http://www.ucl.ac.uk/library/docs/retention-schedule.pdf

7.5. Users may not, under any circumstances, monitor, intercept or browse other users' email messages.

UCL reserves the right to inspect, copy and/or remove user data in order to investigate operational problems or for the detection and investigation of suspected misuse. This includes the authorized interception and monitoring of communications as provided for by The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, made under the Regulation of Investigatory Powers Act 2000.

For example, monitoring of user accounts might occur if the University has reason to believe that its computer facilities were being misused to send unsolicited commercial emails.

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

UCL reserves the right to access and disclose the contents of a user's email messages, in accordance with its legal and audit obligations, and for legitimate operational purposes. UCL reserves the right to demand that encryption keys, where used, be made available so that it is able to fulfil its right of access to a user's email messages in such circumstances.

For the avoidance of doubt, this section does not preclude third parties who operate services on behalf of UCL from carrying out lawful monitoring and disclosure on their systems and networks.

7.6. Any device holding mail messages, email addresses (or any other confidential material) must be password protected.

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.

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	**3 Appropriate Use of UCL Email Services** ***Replaced*** *“on UCL business”* ***with*** *“for UCL related activities.”*
	Added *“3.6 The Information Security Group (ISG) may use email to test user susceptibility and to improve security awareness.”*
	4 Email Servers ***Deleted*** *“Departmental”* ***Replaced*** *“Information Systems”* ***with*** *“ISD”*
	5 Viruses ***Added*** *“and other malware”* ***to the heading*** *“Viruses”* ***Added “****or other malware****”*** **to** *“… of computer viruses or other malware by email.”* ***Deleted*** *“central or departmental” from “routed …via central or departmental mail ..”* ***Replaced*** *“hubs”* ***with*** *“servers”* ***Replaced*** *“virus”* ***with*** *“malware”* ***Added*** *“Systems must run up-to-date anti-malware software where available. All desktop systems should have anti-malware software installed and kept up to date; the operating system must also be patched regularly.”*
	7.4 ***Deleted*** *“There is no UCL policy on retention of email.”* ***Added*** *“Ex.-staff email will be deleted one year after they leave UCL unless otherwise authorised. For further advice see the UCL Records Management retention schedule available here: http://www.ucl.ac.uk/library/docs/retention-schedule.pdf”* *7.6* ***Replaced*** *“personal organizer, etc.”* ***with*** *“device”* ***Replaced*** *“should”* ***with*** *“must”*
	8 Status of this document ***Replaced*** *“Information Strategy Committee”* ***with*** *“Information Risk Governance Group”*

Approvals

Endorsed by the Information Strategy Committee	**1-Dec-2009**
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**