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.

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