Information Security Policy

University College London

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

There are circumstances where UCL may monitor or record communications made using its computer and telecommunication systems, or examine material stored on those systems. This document sets out UCL's policy in respect of such activity.

It is important to be aware of the distinction made between:

intercepting information - email messages being sent, for example, or watching the web pages visited - here the relevant law is found in the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBPR);

to prevent or detect crime;

to investigate or detect unauthorized use, including the use of systems outside UCL;

to ensure the effective and authorized operation of systems;

to establish the existence of facts necessary to ascertain compliance with regulatory or self-regulatory procedures, or to ascertain or demonstrate standards

for other lawful purposes as set out in the relevant legislation;

Stored material (including electronic mail) may also be examined for these purposes. In addition, UCL may access stored material in the event of an urgent need (see section 7).

UCL may also monitor but not record:

received communications to determine whether they are business or personal communications;

'Authorized use' of UCL facilities is defined in section 2 of the UCL Computing Regulations (see references below). It should be noted that although reasonable personal use of facilities is permitted, excessive use that disrupts or distracts an individual from the efficient conduct of UCL business, or involves accessing or sending unlawful or offensive material (for example, obscene, discriminatory or abusive material), is prohibited; and, consequently, monitoring may take place to detect or investigate such behaviour.

3.1. Monitoring for operational reasons

Most providers of IT services within UCL routinely monitor their systems to ensure that they are performing properly. This reflects standard good practice, and normally involves only aggregate anonymous data that does not identify individuals or the contents of their communications. Information Systems, for example, records the number of email messages passing through its servers each day, and the time it takes to deliver messages, to help with capacity planning. This type of monitoring does not fall within the RIPA, as it does not involve interception, and by virtue of not identifying individuals, it does not trigger laws relating to personal privacy.

The following message should be displayed wherever UCL systems are used (e.g. labels on screens):

Communications, i

Document Control Sheet
Revision History

14.02.2017

TBD

14.02.2017	*Replaced all occurences of "Computer Security Team" with* "Information Security Group"
	Replaced all occurences of "CST" with "ISG"
	Replaced "Information Strategy Committee" with "Information Risk Governance Group (IRGG)"