



## ■ Freedom of Information

There are guidelines for staff regarding FOI legislation at <http://www.ucl.ac.uk/foi/staff-guidelines/>

## ■ Institutional Firewall

UCL has an Institutional Firewall which helps to protect UCL from damaging activity on the Internet and the Internet from abuse originating within UCL.

## ■ System managers

System managers and network administrators should be familiar with the code of practice at [www.ucl.ac.uk/cert/swg/policy/Charter.html](http://www.ucl.ac.uk/cert/swg/policy/Charter.html)

## ■ For further information

This user guide is a summary of some of the most important elements of UCL's information security policy. The full set of documentation may be found at [www.ucl.ac.uk/cert/swg/policy.html](http://www.ucl.ac.uk/cert/swg/policy.html)

The documents of relevance to most people are the UCL Computing Regulations and UCL's Data Protection Policy.

If you would like to discuss any matters relating to the policy, or any of the supporting documents, please contact the Computer Security Team in the first instance, or UCL's Data Protection Officer. Contact details are given on the rear page of this leaflet.

## ■ How do I report problems?

**All suspected computer security problems should be reported to the UCL Computer Security Team.**

To contact the team, send an e-mail to:

**[cert@ucl.ac.uk](mailto:cert@ucl.ac.uk)**

or call 020 7679 7338 (UCL internal extension 37338).

You should not send very sensitive material via e-mail; please phone for advice.

**Any suspected or actual breaches involving personal information must be reported to the Data Protection Officer:**

**[data-protection@ucl.ac.uk](mailto:data-protection@ucl.ac.uk)**

or call 020 7679 7783 (UCL internal extension 37783).

**Breaches of physical security (such as the theft of equipment) should be reported to UCL Security:**

020 7679 2098 (UCL internal extension 32098).

# UCL SECURITY POLICY



## User Guide to UCL's Information Security Policy

## ■ What's it all about?

**UCL's information security policy sets out to ensure that our computing systems, and all the information held on them, are adequately protected against loss and misuse, and that protection is provided in a cost-effective way.**

The policy applies to staff and students alike, and to anyone else who has been authorized to use our facilities. It has been endorsed by UCL's Information Strategy Committee.

## ■ What do I need to do?

First of all, **be aware of our computing regulations**. As well as considering how we use computers in our work, they define - and allow for - reasonable personal use of UCL's computer systems. However, reasonable personal use **does not include commercial activity**, activity which breaks the law, is likely to cause offence, or which because of volume or frequency distracts from work. Personal use must not cause problems for other users, add significantly to running costs, or risk bringing UCL into disrepute.

**Breaches of regulations can result in serious disciplinary action.** If you're not sure about something you want to do, check first with your supervisor, tutor or manager.

You should **know what to do in the event of a security problem**. Identify the person who is responsible for the computers that you use. If you have a problem, or notice something you think is wrong, report it. If you can't find anyone to report to, contact UCL's Computer Security Team. The team's details are given below. Do not try to investigate security problems yourself unless you are explicitly authorized to do so.

Continued in next column

## ■ What do I need to do? (continued)

If you want to attach any device to the UCL computer network, you'll also need to **know who your departmental network administrator is**. Speak to them before you try connecting your equipment: at the very least, you'll need to ask them for information to configure the network settings on your computer. Approval from UCL's Computer Security Team is needed if you wish to connect a new wireless access point to the UCL network.

If you will be **looking after your own computer, or managing other systems in your department**, then familiarize yourself with the duties of system custodians. You'll find them set out in full on the information security policy web page (see the reference below): you must keep your computer's software and operating system up-to-date; ensure you're running appropriate anti-virus software; restrict access to authorized users only; and make sure that your departmental network administrator has a record of the machine's details, so that in the event of problems we can contact the right person quickly. You may need training for this! Tell your supervisor/manager if you feel you do.

If you intend to **collect or process any personal information about living people**, read UCL's data protection policy, or speak to the Data Protection Officer. Computers that hold sensitive information will need higher levels of protection than those that do not. Remember also that e-mail isn't a very secure medium, and take special care when drafting messages which reference personal information or sensitive matters. Use an official e-mail account for UCL business; avoid free 'webmail' accounts for such purposes.

Finally, it's important to realize that **anyone who is given access to our computer systems is being placed in a position of trust** – so we all have some responsibility for protecting UCL's information systems. Don't share your passwords with your friends, relatives or colleagues, or take part in any activity that may jeopardise our security.

## ■ What is my department doing?

Departments are required to identify all computer systems and any critical or sensitive information stored on them. A custodian must be nominated for each system with responsibility for making sure it is kept secure and up-to-date. In most Departments, custodians will be responsible for more than one system, and will assist the Head of Department in preparing periodic assessments of the security of the systems under their charge for the Information Strategy Committee.

Departments must also nominate a departmental network administrator who will allocate Internet Protocol (IP) addresses to individual machines and register them in the Domain Name Service (DNS). Approval from UCL's Computer Security Team must be obtained before connecting any wireless access point to the UCL network. Where any other type of access point is introduced into the network infrastructure, UCL's Network Group must be notified. Regardless of the technology, it may become necessary to determine which system had use of a particular address at a given time; appropriate records should therefore be kept for six months.

**All monitoring of computer systems and networks must be authorized.** Be aware that the legal definition of monitoring is broad; it includes prevention or detection of misuse and many activities carried out routinely by system and network administrators. Penalties for unauthorized monitoring are severe (possibly involving imprisonment). UCL monitoring policy is at [www.ucl.ac.uk/cert/swg/policy/Monitoring.html](http://www.ucl.ac.uk/cert/swg/policy/Monitoring.html). All staff and students should be aware that their computer usage may be monitored.

Departments disposing of old computer equipment should ensure that no sensitive material is left on them before they are re-cycled. All disks (including removable media) must be thoroughly erased – see [www.ucl.ac.uk/cert/secure\\_disposal\\_guidelines.pdf](http://www.ucl.ac.uk/cert/secure_disposal_guidelines.pdf) for details. If the computers are to be re-used, similar care should be taken to respect the terms of any software licences.