What is my Department doing? (cont'd)

- All monitoring of computer systems and networks must be authorised. 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 unauthorised monitoring are severe (possibly involving imprisonment). All staff and students should be aware that their computer usage may be monitored (see Links section below).

- Departments disposing of old computer equipment should ensure that no sensitive material is left on them before they are recycled. All disks (including removable media) must be thoroughly erased – see disposal guidelines below. If the computers are to be re-used, care should be taken to respect the terms of any software licences.

Links

Freedom of Information – There are guidelines for staff regarding FOI legislation at **www.ucl.ac.uk/foi/guidelines**

System managers – System managers and network administrators should be familiar with the codes of practice at **www.ucl.ac.uk/informationsecurity/policy/internal-policy/Charter** and **www.ucl.ac.uk/informationsecurity/policy/internal-policy/Custodians**

Monitoring Policy
www.ucl.ac.uk/informationsecurity/policy/public-policy/Monitoring

Disposal Guidelines
www.ucl.ac.uk/informationsecurity/secure_disposal_guidelines

Wireless Access Point Registration Form
www.ucl.ac.uk/is/network/wireless/departmental/registration.php

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

How do I report problems?

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

UCL Information Security Group:
email: **isg@ucl.ac.uk**
tel: **020 7679 7338 (37338)**

Data Protection Office:
email: **data-protection@ucl.ac.uk**
tel: **020 7679 5681 (45681)**

UCL Estates Security (physical):
tel: **020 7679 2108 (32108)**

PCI DSS Card Security – Finance & Business Affairs:
email: **uclonlinestore@ucl.ac.uk**
tel: **020 7679 1663 (41663)**

For further information

Full documentation can be found at:
www.ucl.ac.uk/informationsecurity/policy

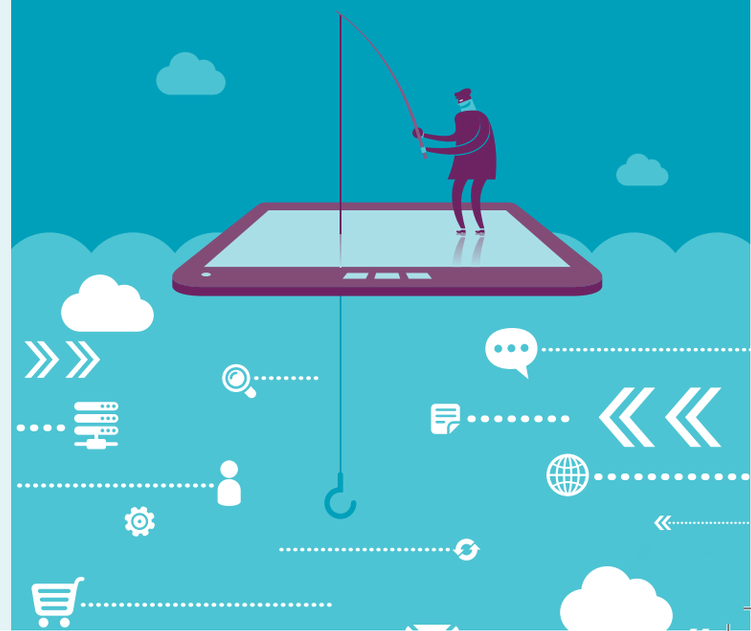
Try our Information Security Awareness course at:
https://moodle.ucl.ac.uk/course/view.php?id=26205

2015 / 2016

UCL INFORMATION SECURITY GROUP

UCL

User Guide to UCL's Information Security Policy



What's it all about?

UCL's Information Security Policy sets out to ensure that the information we use for teaching, learning and research (either directly or indirectly), is adequately protected in terms of confidentiality, integrity and availability, and that the protection is cost-effective.

The policy applies to staff and students alike, and to anyone else who has been authorised to use any facilities in UCL. It has been endorsed by UCL's Information Services Governance Committee.

Breaches of the regulations can result in disciplinary action, if you're not sure about something check with your supervisor, tutor or manager first.

What do I need to do?

Computing Regulations

- First of all, be aware of our Computing Regulations (link at the end of this leaflet). As well as covering the use of computers for our work, they allow for – and define – reasonable personal use of UCL's computer systems. Reasonable personal use does not include commercial activity, use which breaks the law, is likely to cause offence, or (because of volume or frequency) distracts from work. Personal use must not cause problems for other users, significantly add to running costs, or risk bringing UCL into disrepute.

Payment Card Data

If your department is taking/intending to take credit or debit card payments, you must contact Finance and Business Affairs (contact details overleaf).

Incidents

- 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 Information Security Group (details are at the end of this leaflet).

- Do not try to investigate security problems yourself unless you are explicitly authorised to do so.

Everyone's Responsibilities

- If you want to attach any device to the UCL computer network, you 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 Information Security Group is needed if you wish to connect a wireless access point to the UCL network.

- If you are looking after your own computer, or managing other systems in your department, familiarise yourself with the duties of a system custodian. You'll find them set out in full on the Information Security Policy web page (see the reference overleaf). You must keep your computer's applications and operating system up-to-date; ensure you're running appropriate anti-virus software; restrict access to authorised users only; and make sure that your departmental network administrator has a record of the machine's details, so that in the event of a problem we can contact you quickly. You may need training for this! Tell your supervisor/manager if you feel you do.

- It is important to realise that anyone who is given access to our computer systems is being placed in a position of trust – 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.

Data Protection

- If you intend to collect or process any personal information about living people, you need to 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 email isn't a secure medium, and take special care when drafting messages which contain personal information or refer to sensitive matters. Use an official email account for UCL business and avoid free 'webmail' accounts for such purposes.

Departmental Responsibilities

- 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 in their charge.

- 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). Where any other network device is to be introduced into the network infrastructure, UCL's Network Group must be notified (see Links section). Regardless of the technology, it must be possible to determine which system had use of a particular IP address at a given time; appropriate records should therefore be kept for six months.

Continued overleaf