When disposing of computer generated information (defined as personal or confidential data under the Data Protection Act), users must ensure that standards of confidentiality are applied to ensure that data is destroyed appropriately.

All storage media and hard drives should be disposed of in a manner that complies with the Disposal of Computers and Computer Media Policy to prevent any breaches of confidentiality.

ICT facilities supporting critical or sensitive business activities should be housed in secure areas with appropriate access and security controls, for example, restricted swipe card entry and alarm system.

Additional protection such as uninterruptible power supplies (UPS), air conditioning and humidification units should be used, where needed, to protect against environmental damage and fluctuations of power supply.

Contacts

These guidelines are intended to complement, but not replace the Trust's formal policies and procedures regarding Information Security.

The latest Information Security documents, policies and leaflets are available for download from the Trust's Information Security Intranet site:

http://intranet/infosec/

If you have questions regarding the contents of this leaflet please contact:

ICT Services Helpdesk

City Hospital Campus

Telephone Extension: 47777

QMC Campus

Telephone Extension: 69000

David Cadwell

Information Security Adviser

david.cadwell@nuh.nhs.uk

Neil Mullinger

Deputy Information Security &
Data Protection Adviser

neil.mullinger@nuh.nhs.uk

Nottingham University Hospitals NHS
NHS Trust

Information Security

Hardware & Software Guidelines

This leaflet provides guidance on acceptable use of hardware and software

Version 1.3 — Updated 22-06-06

Software

Software must not be installed by users because of the risk of virus infection and insufficient licensing.

Adequate licences must be maintained for all installed software and the licences should be stored in a secure location.

If you find some software that may be of use to your department please discuss it with your manager.

It is important than trial software is either removed or licences are purchased once the trial period has expired.

Installation and removal of software should in most cases be conducted by ICT Services.

Master copies of software, backup tapes and manuals should be kept in a locked, secure location and be protected from environmental damage such as fire, flood and extreme temperatures and humidity.

Backups of master disks should be taken (subject to licence agreement) and used to install applications.

Master copies should not be in general use unless copyright forbids making backups.

Back-up of important information and data should be conducted on a regular basis.

Operating systems should be kept up to date and new security patches should be applied to reduce the risk of security breach.

Staff who have access to software which contains confidential information must always ensure that the system is secured when unattended, this can be achieved by ensuring the computer is ‘locked’ or by logging off the network.

Confidential information should not generally be kept on PC’s, but in those circumstances where it is, steps should be taken to ensure the information is kept secure. This could involve the use of encryption software. For more information on this, please contact the ICT Services Helpdesk.

Staff may not sell, rent, sublicense, lend, transmit, distribute, give, or otherwise convey or make available software or an interest therein to any unauthorised individual or entity.

Hardware

No modifications should be made to Trust owned ICT equipment by unauthorised staff, upgrade requests must have management approval and the actual upgrade work should only be performed by authorised members of staff e.g. ICT Services.

All Trust owned ICT equipment should be listed on an asset database and be security marked.

Additional security devices are available for purchase either with a new system or as separate items.

These devices should be seriously considered for equipment that is used in public, open access areas and for laptop computers.

In general, apply security precautions relative to the risks that may effect the equipment. For more information or advice on what to use, please contact the ICT Services Helpdesk.

Network cabling should be protected against damage and interception by the use of enclosures and ducting.

Switches, hubs and other network hardware should be secured to prevent unauthorised alterations.