Always use the absolute minimum amount of patient identifiable information (e.g. use a hospital number instead of the name) wherever possible.

Software must not be installed by users as this introduces a higher risk of computer virus infection and may also breach copyright restrictions.

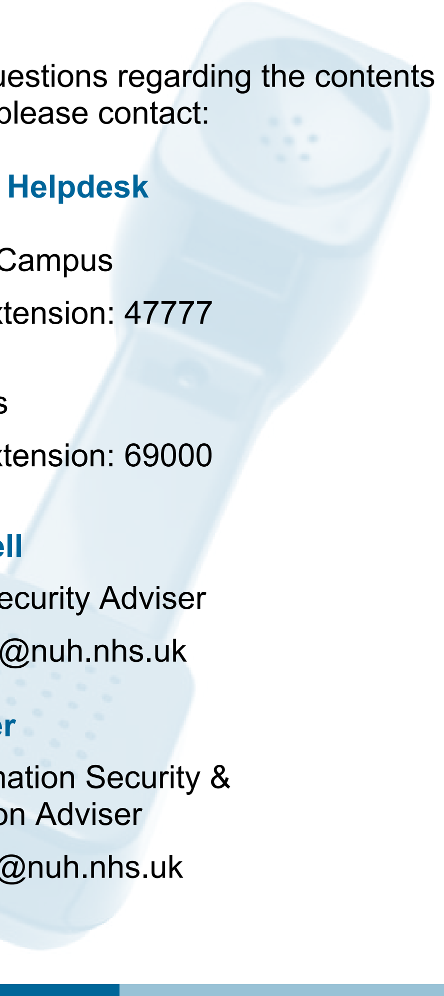
If software is required then it should be normally be installed by ICT Services.

User created file shares are not permitted, if a share is required a request should be logged with the ICT Services Helpdesk for one to be set up.

Redundant media such as CD’s and computer hard drives must be disposed of in a way that complies with the Disposal of Computers and Computer Media Policy.

Backup tapes and master disks should be stored in a locked cabinet protected from environmental dangers such as fire, flood and extremes of temperature and humidity.

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

Information Storage & Virus Protection Guidelines

This leaflet provides guidance on virus protection and the secure storage of information

Version 1.3 — Updated 11-05-2006

Virus Protection

The threat of damage to important business information and sensitive patient data from malicious computer viruses is increasing as the number of personal computer (PC) based applications grows.

This guideline aids staff on applying good practice to avoid viruses and how to handle them when encountered. It is a requirement of the Trust that all Trust PC's have virus-scanning software installed, active and updated regularly.

The Trust only allows approved software to be loaded on its PCs.

A frequent source of computer viruses is removable media such as floppy disks or CDs.

In the majority of cases viruses are transmitted to PC's by one of the following routes:

- Free disks or CDs from magazines
- Pirate software or games, especially those downloaded from file sharing programs.
- Electronic Mail
- CD's brought into work from home computers.

Many types of viruses exist including:

- **Trojan Horses**
  These can log everything you type and allow remote access to your machine.
- **File Viruses**
  Mostly pretty harmless but some types can erase all data on a hard disk.
- **Worms**
  Will attempt to replicate by sending copying itself to every user in the address book or via network connections.
- **Macro Viruses**
  These can infect documents made in programs that use macro's such as word, excel and access.

The effects of viruses can vary greatly, they may just produce a message on screen or could in the worst case completely corrupt or delete all the data on the hard disk.

If you receive a virus warning by email, please do not send it out to other people, contact the ICT Services Helpdesk for advice. Many of these warnings are hoaxes!

We have some of the best virus protection available, but if you suspect your PC has been infected with a virus, please inform the ICT Services Helpdesk immediately.

Information Storage

Access to patient and staff identifiable information should be restricted only to those authorised to see it.

Documents and files should be stored in the users network account, this is a secure location provided passwords are kept secret and the account is not left unsecured while unattended.

Confidential information should never be stored on a local hard disk unless it is is secured.

To achieve an acceptable level of security for confidential information the data must be password protected and the physical equipment must be in a secure location.

Information should be protected by clearly defined and controlled backup procedures.

Equipment or sensitive data should not be taken off site without management authorisation, if permission is granted then the information and equipment should be secured e.g. do not leave in your car.

All PC's, laptops and other portables should have a designated owner who is responsible for the equipment and the information that is stored upon it.