Information security is achieved by implementing a suitable set of controls, which include policies, practices, procedures, organisational structures and software functions.

Increasingly, organisations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood.

Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

Some aspects of information security are governed by legislation.

The most notable U.K. Acts are:

- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- Data Protection Act (1998)

Additionally, staff are under a common law obligation to preserve the confidentiality of this information.

Information security needs the active participation of all employees in the organisation to ensure that staff and patient information is kept secure and confidential.

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 Security & Password Guidelines

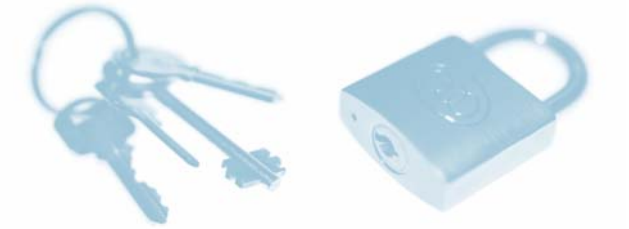
This leaflet defines Information Security and gives advice on creating secure passwords.

Version 1.3 — Updated 04-05-2006

Password Security

Your password is your main protection against someone else using your account and acts as a barrier against someone else accessing unauthorised information.

Passwords are the keys that open electronic doors and should be treated with as much care as a bunch of physical keys.



Normally you should do your best to memorise passwords, but they can be written down provided they cannot be recognised as such e.g. do not write down ‘password to cardio system’ next to it.

Passwords that are written down should be secured. This could be accomplished by locking the paper away in a drawer or keeping them password protected on a PDA.

No matter how much money is spent on sophisticated network technology to prevent unauthorised access to data, a weak or poorly concealed password has the potential to bypass it all.

Remember that all activity on your account is deemed to have been made by you and unauthorised access is a criminal offence.

Follow the advice here and help us to keep patient and staff data secure and protected from unauthorised access.

What you should do:

- ✓ Change your password regularly
- ✓ Add some numbers to your password
- ✓ Try to add characters such as £ - * ^ { / | into your password.
- ✓ Choose a password that cannot be easily guessed.
- ✓ Always keep passwords secret.
- ✓ Change your password immediately if you suspect someone knows it.
- ✓ Log out or lock the computer when it is unattended.
- ✓ Try to use phrases to help make a complex and more secure password. For example; ‘One day I will visit the US’ can become ‘odiwvtus’ by using the first letter of each word.
- ✓ Make sure nobody is watching you type your password.

What you should NEVER do:

- × Do not create a password that is easy to guess, avoid personal information such as car registrations, names of people or pets, hobbies or interests.
- × Do not share passwords or system accounts, if a person needs access to something they do not have their own account for, they must speak to their manager to get access.

Information Security

Information is an asset which, like other important business assets, has value to an organisation and consequently needs to be suitably protected.

Information security measures are designed to protect information from a wide range of threats in order to ensure continuity and minimise damage.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means.

Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security can be defined as protecting the confidentiality, integrity and availability of data and information.

Confidentiality:

Access to information is confined only to those with specified authority to view that data.

Integrity:

Safeguarding the accuracy and completeness of information and software.

Availability:

Information is delivered to the right person, when it is needed.