Misuse of the email system is an abuse of Trust resources and is therefore a disciplinary offence.

Users with access to national email should note that misuse of this system breaches the Trust's Code of Connection to NHSnet and could result in the removal of this facility.

Staff should remember that emails are legal documents and could be used as evidence in court.

Never email confidential information or data out of the Trust unless it is password protected and the recipient has a right to see that information.

**System-wide Emails**

As a rule of thumb system-wide emails should only be sent if the contents of the message meets one of the following criteria:

- Staff need to know something in order to do their job.
- The Trust needs to inform staff of an issue.
- A department is seeking or offering help.

In all cases the message must be relevant to the majority of users.

## 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

## Internet & Email Guidelines

This leaflet provides guidance on the acceptable use of Electronic Mail and the Internet.

Version 1.3 — Updated 23-06-06

## Internet Guidelines

IT facilities such as the Internet and email have been provided by the hospital primarily for business purposes. Limited personal use of these facilities is permitted e.g. during lunch breaks and after work hours, provided you have management approval.

You should be aware that a range of monitoring is conducted on Internet usage. This includes time spent on the Internet and a list of visited websites. Logs of Internet usage are used to investigate allegations of misuse.

The Internet should not be used unless the computer has virus checking software installed, active and kept updated.

All downloaded files should be virus checked to protect against contamination before they are used.

If a web page cannot be accessed it is possible that the site has been added to the ban list. Sites that are added to this list include ones that contain offensive content i.e. pornographic, terrorist, racist etc.

Large downloads i.e. files in excess of 10 Mb, should normally be downloaded in quiet periods of the week to preserve bandwidth.

The best times to download large files are before 9.00 am and after 5.00 pm. This is when Internet traffic is at its lowest.

If you require a program from the Internet please inform your line manager.

You should not download or install software unless authorised to do so. This is to protect against virus infection and ensure all software is correctly licensed. All trial software must be removed once the trial has expired.

The Internet must not be assumed to be secure. Confidential information or data must never be transmitted over the Internet unless the data or information is encrypted.

Staff should note that failure to adhere to the above guidelines and/or abuse of these facilities would render individuals liable to their access being withdrawn and disciplinary action may be taken against them in accordance with the Trust's Disciplinary Procedure.

## Email Guidelines

Email at work is primarily provided for work purposes. Staff may use the system for personal mail provided it is not excessive, is in accordance with Trust policy and has management approval.

All incoming email-attached files should be virus checked before use to protect against virus infection.

Always treat attachments on emails from outside the Trust with caution, especially those ending with extensions such as .exe, .bat or .com. If in any doubt, contact the ICT Services Helpdesk for advice.

Do not keep or forward junk mail and never reply to it. If you receive junk mail from the same people on a regular basis, you should contact the ICT Services Helpdesk.

Remember that storage space is finite. If you get a warning message to clean out your mailbox you should do so, if not, the system may automatically lock you out.

Auto forwards should not be set to send mail to external accounts (University email accounts are classed as external) where there is the possibility of any personal or confidential information being sent out onto the Internet.

As mentioned before, the Internet is not considered to be a secure transport medium.

Setting an auto forward to a ‘trusted’ email address is permissible, e.g. to an email account of another employee on the Trust’s network. If you require any assistance with setting an auto forward, please contact the ICT Services Helpdesk.