IINFORMATION GOVERNANCE TOOLKIT POLICIES: INTERNET AND EMAIL

What is the internet?
The internet is a worldwide communications network linking together computer networks and millions of users across both public and private telecommunications lines. The internet and the World Wide Web (www) are not the same thing - the web is a collection of documents and other resources accessible via the internet, along with other services such as email.

What is email?
Email is an electronic method of writing, sending, receiving and storing messages via either internal networks or via the internet. Electronic files and other documents can be attached to email messages.

What are the risks?
Because of the open nature and ready availability of email and internet services, there are potential dangers associated with its use. These could arise from malicious intent, carelessness, complacency or misuse.

Therefore most organisations develop policies and guidelines to help users make the most effective use of the facilities, whilst at the same time minimising any associated risks.

The internet and email are the most common source of computer viruses, malware, spyware and other malicious code. (For more help on these topics see Good practice guide - safe computing.)

Infected files could be unwittingly downloaded from the internet, or contained in email attachments. Any deliberate file downloads must also comply with relevant copyright or licensing regulations.

It is important to note that email messages carry the same legal status for the organisation as more conventional paper memos and letters, therefore particular care should be taken with the content wording.

Furthermore, it is very easy for an email message to be forwarded on to additional recipients who were not on the original distribution list, without your knowledge or consent, so again, care must be taken with the overall content and confidentiality of the topics being discussed.

Any personal, sensitive or confidential information (either yours or someone else's) should not be shared or sent over the internet or by email unless appropriate confidentiality and security procedures are in place; otherwise this may be in breach of the Data Protection Act 1998.

Misuse of internet and email may contravene one or more legislative frameworks, including (but not limited to) the Data Protection Act 1998, Computer Misuse Act 1990, Electronic Communications Act 1990, Freedom of Information Act 2000, the Law of Copyright. The implications of these and other regulations should be clearly understood.

South
collective thinking

IINFORMATION GOVERNANCE TOOLKIT POLICIES: INTERNET AND EMAIL

Using the internet

Use of the internet using NHS computer equipment and networks for work related research and communication is generally acceptable, however this usage may be monitored. This monitoring may include tracking which internet sites have been visited to ensure that subject matter and content is deemed to be appropriate.

As you browse a website, files may be passed to your computer known as 'cookies'. These are generally harmless data files created by the site, containing information about you, the network you are using, your software, or your site settings or preferences, so that the site can 'remember' you the next time you visit. However, there are some types of files that can cause problems.

With these things in mind, it is important that you only access trusted sites that are managed by organisations that you know. Access to the more unsuitable sites may automatically be blocked; for example, sites which contain material of a pornographic, racist, or otherwise inappropriate or offensive nature. However access to sites should not be regarded as legitimate just because it is possible to get to them.

'Search enginess such as Google or Yahoo are commonly used to find documents and articles on the internet. Typically you would type in a few keywords or a short phrase that describes what you are looking for into the query box, then the search engine will provide a list of links to websites that it thinks might be of interest to you. However be aware that it is also likely to also find many other items that will be of little or no interest as well! The trick is to construct your query as specifically as you can.

Using email

Most people now have an email address - either personal or work related - which will look something like my.name@nhs.net. Most email systems include an electronic address book - where you can save email addresses for future use - and the ability to create folders for saving and organising your messages.

Key advantages of using email over paper include:

- saving time in copying and distributing information
- automatic storage of sent messages and documents
- sharing information quickly and easily.

However, the informal nature of emails may encourage people to send messages which they might not otherwise consider passing face to face or via the telephone.

In terms of security, unless your email system is otherwise protected, you should consider an email to be on a par with sending a postcard, ie there is a possibility that messages may be read by anyone. Many email systems use a messaging protection system known as 'encryption' to ensure that confidential or sensitive messages can only be opened by known and authorised recipients. This is more akin to sending a letter in an envelope marked 'Private & Confidential'. Before sending any confidential material you should make sure you understand your organisation's policy and security requirements.

IINFORMATION GOVERNANCE TOOLKIT POLICIES: INTERNET AND EMAIL

Remember:

Do

- make sure you have read and understood the internet and email policies relevant to your organisation
- scan any email attachments for viruses before you open them
- only address emails to people who really need to know about the subject
- include a relevant title for your email message
- make sure you are aware of confidentiality and data sensitivity issues before sending messages
- be sure that information published on a website is accurate and up to date before using it.

Don't

- access websites that may contain inappropriate or offensive material
- download files or open email attachments without being absolutely certain that you can trust the sender and the content
- circulate emails to everyone in your address book just because you can
- send large attachments to multiple recipients
- send or forward junk mail, chain letters or virus warnings - these may be hoaxes or dangerous.