Acceptable use of ICT policy

Introduction

This policy forms part of the overall Information governance policy.

By signing to say that you have read and understood this policy, you have agreed to the code of conduct as described in this document. Failure to comply may result in disciplinary action, which could ultimately lead to dismissal or criminal prosecution.

The purpose of this policy is to clearly explain what is

- acceptable and
- unacceptable use of electronic mail

General guidelines

User names and passwords

Each user is responsible for maintaining the security of their individual login and password. Staff must not share their user name or password with anyone. Passwords must be changed on a regular basis. If a breach of security is recorded under your login, you are responsible for the breach and disciplinary action may be taken against you.

Computer protection

Do not leave a computer logged on and unattended. If a computer is left logged on and unprotected another person can send and receive messages in your name. Ensure that password protected screen savers or other mechanisms prevent the use of your identity by a third party.

Using electronic mail Acceptable use of electronic mail

Electronic mail (e-mail) and internet is to be used for work related purposes. Limited personal use of e-mail is allowed provided it does not interfere with your work nor expose the organisation to any expense or liability. Your manager may stop you from using e-mail for personal use if you abuse this privilege. You are required to act in accordance with your manager's guidelines.

Unacceptable use of the electronic mail

You are not allowed to e-mail material that it liable to offend. Material that is liable to offend includes

hostile text or images related to gender, ethnicity, race, sex, sexual orientation, age, religious or political convictions and disability. You are not allowed to e-mail material that has a criminal or terrorist content. You are not allowed to send or participate in the dissemination of chain or joke e-mails. Any breach may be treated as a disciplinary offence, which could ultimately lead to dismissal or criminal prosecution.

Patient/Personal identifiable data

Patient identifiable data can only be sent by e-mail in a manner approved by the Caldicott Guardian. The most secure way of sending personal identifiable information electronically is from one nhs.net email account to another nhs.net email account, in line with recommendations from Connecting for Health and the Department of Health. The NHSmail email service is unique because mail is encrypted in transit. This means that it is acceptable to use the service for the exchange of patient information between NHSmail accounts, (http://systems.hscic.gov.uk/).

Advertising

The e-mail system is not intended for commercial or personal advertising.

Virus protection and detection

All computers are protected with anti-virus software. However, this only works for a known virus. If you receive an e-mail from an unknown source, think before you open the e-mail.

Hoax e-mails

If you receive an e-mail that you think is from a suspicious source delete it. E-mail is not the only method of communication and if you mistakenly delete the email, the source will re-contact you somehow.

E-mail content

E-mail is treated by a court of law in the same way as spoken or written statements. You must therefore take care with the contents of your e-mail as the contents may form a legally binding document.

Distribution lists

E-mail distribution lists should only contain addressees who are appropriate recipients of the e-mail content. E-mail should not be sent out to a large number of people unless essential as you could be wasting people’s time and causing possible disruption to services. Do not ask for acknowledgements from distribution lists.

Unacceptable use of the internet

You are not allowed to access, display or download any material that is liable to offend. Material liable to offend includes hostile text or images related to gender, ethnicity, race, sex, sexual orientation, age, religious or political convictions and disability.

You must not use the internet, to attempt any unauthorised access to resources (hacking). Nor are you allowed to access hacker websites as some sites contain traps, which may trigger malicious programmes when an Internet page is accessed.

The Internet should not be used for browsing, downloading and/or posting (as appropriate) any of the following:

- Content that expresses personal views about subjects unrelated to and inappropriate

for a productive workplace;

- Accessing sites that relate to or provide information on criminal or terrorist activity;

and/or

- Accessing sites that the whole prime function is to provide offensive material. Posting,

downloading or viewing pornography may constitute a criminal offence and is likely to be viewed as gross misconduct warranting summary dismissal.

- Downloading of music, audio and video, not related to work.

Any breach may be treated as a disciplinary offence, which could ultimately lead to dismissal or criminal prosecution.

Unintentional breaches of security

If you accidently find yourself connected to a site, which contains unacceptable material, you must disconnect from the site immediately and inform your manager and the Security lead.

Downloading of files and material from the Internet

If you have authority to download files the following rules apply: It is a breach of security to download files which disable the network or which have the

purpose of compromising the integrity and security of the networks and file servers.

- To intentionally introduce files which cause computer problems could be prosecutable

under the Misuse of Computers Act 1990.

- Where permitted, file downloads must be done in accordance with laws that protect

copyright, designs and patents. Some materials on the Internet are copyright works or trademarks belonging to third parties. You must not print or download or in any way attempt to reproduce or disseminate any document or material from the Internet unless you are sure that it is not protected by copyright or trade mark law. You should check with the Security Lead if you are in any doubt in any particular case.

Joining chat rooms and news group

If you join a chat group or news group related to your work, you are expected to conduct yourself in a professional manner. Be courteous and inoffensive. Unless you are authorised to do so, you are not permitted to write or present views on behalf of Peninsula Ultrasound Ltd.