Walton Centre

Acceptable Use

Document History

Date	Version	Author	Changes
01/10/2004	1.0	A Cobain L Wyatt	
06/01/2005	1.1	L Wyatt	Update of procedure information
31/03/2005	1.2	L Wyatt	Update of Trust Procedure

Table of Contents

1. Introduction

Information and information systems are important assets and it is essential to take all the necessary steps to ensure that they are at all times protected, available and accurate to support the operation and continued success of the Trust.

The Trust acknowledges that we must demonstrate to our stakeholders our commitment to, and delivery of, effective information security.

The aim of the Trust Security Policy, Standards and Guidelines is to maintain the quality, confidentiality, and availability of information stored, processed and communicated by and within the Trust. These policies, standards, guidelines are used as part of the information security management system (ISMS) within Trust.

To facilitate effective working the Trust allows all employees' access to appropriate information systems and technology, including the Trust network, and email. However, with this comes risks to the Trust. This standard, therefore, sets out the standards applicable for the use of information and information systems within the Trust.

This standard applies to all staff, whether permanent, part-time or temporary. It applies also to contracts granted access to Trust information and information systems.

2. Responsibilities Within This Standard

All employees using IT equipment, the internet or e-mail have responsibilities with regard to this standard. Particular responsibilities within the standard are defined as:-

Review and Maintenance	Head of IT
Approval	Information Security Forum
Local adoption	Line Managers
Compliance	All users

3. IT Equipment and The Network

3.1 Context

The Trust has an established IT infrastructure which permeates all areas of the organisation allowing users access to information in order allow them to do their jobs effectively. This equipment is becoming increasing sophisticated with greater and greater functionality; examples would include the increasing incorporation of CD / DVD writing equipment in standard pc's. This could also include the connection of USB storage devices and PDA's. However, with this comes a greater risk of misuse.

3.2 Business Use

Equipment is provided on the basis of business need. Use of the equipment provide for business purposes is acceptable only where such use falls within the normal day to day remit of the individual.

In particular, the following guidelines will must be applied:-

- Users must not in any way cause any form of damage to the Trust's IT Systems, nor to any of the accommodation of services associated with them.
- Users must adhere to the terms and conditions of all licence agreements relating to IT Systems which they use including software, equipment, services documentation and other goods.
- Users must not modify any software nor incorporate any part of the provided software into their own work without permission from the designated authority.
- Users must not load onto the IT Systems any software without permission from the designated authority.
- Users must not deliberately introduce any virus, worm, Trojan horse or other harmful or nuisance program or file into any IT Systems, nor take deliberate action to circumvent any precautions taken or prescribed by the Trust to prevent this.

- Users must not delete or amend the data or data structures of other users without their permission.
- Users must not in their use of IT Systems exceed the terms of their registration. In particular they must not connect to any other computing IT Systems without the permission of the designated authority.
- Users of networks and remote IT Systems shall obey any published rules for their use.
- Users must ensure that they start and terminate each session of use of IT Systems in accordance with published instructions.
- Consumables including stationery must be used for the purpose for which they are supplied and their consumption should be minimised as far as is reasonably possible. Used and scrap paper should be disposed of so as to minimise any risk of a breach of the data protection act.
- Users must not interfere with the use by others of the IT Systems; they must not remove or interfere with output belonging to another user.
- The creation, display, production or circulation of offensive material in any form or medium is forbidden.
- Users must take every precaution to avoid damage to equipment caused by smoking, eating or drinking in its vicinity. In particular, smoking, eating or drinking in IT Systems room is forbidden.
- Users must respect the rights of others and should conduct themselves in a quiet and orderly manner when using IT Systems.
- Users must respect published times for access to IT Systems.

3.3 Personal Use

Equipment and systems are provided to users for businesses purposes, however the Trust wishes to encourage users to develop their IT skills and acknowledges that formal training is often best complemented by "trying things out" or personal use. Personal use, however, represents an area of concern not just in the NHS but in all sectors given the risks faced.

It is the Trust view that limited personal use is acceptable but this should be confined to non-business hours and should, at all times, be legal. Further, such use should only be for personal purposes. The use of Trust equipment to support or pursue private businesses is not acceptable.

Some examples of acceptable personal use could include such things as a personal letter to your bank; maintaining or updating CV or completing college assignments.

Similarly, but not exhaustively, some examples of unacceptable use could include the storage of illicit, pornographic or racist material or the use of the equipment to duplicate copyrighted materials such as software or music.

Users must not install personal software on Trust equipment regardless of its nature. Only software which supports Trust business is to be installed and in all instances this must be done by a member of the IT Department.

In all instances, usage can only be acceptable if it is by a Trust employee / contractor. Use of equipment by family or friends is unacceptable regardless of the purpose of use.

4. E-mail

4.1 Context

E-mail is becoming an increasingly essential business tool, facilitating the sharing and dissemination of information between staff and beyond organisational boundaries. While essential to the effective operation of the Trust there are risks to its use as has been demonstrated in highly publicised cases in the media.

E-mail sent over the internet is not secure and as such patient identifiable information should never be sent in this form {For exception see 4.2.2 NHS Mail]

Under no circumstances should Patient Identifiable Information be transmitted by non secure e-mail

4.2 Business Use

4.2.1 Trust E-mail System

The Trust e-mail system is, essentially, a business facility. Users should be aware that e-mail is legally attributable to the Trust in exactly the same way as letters/fax/memos and therefore information, which could be construed as legally binding, should not be transmitted over e-mail.

The content of all e-mail stored on equipment owned by the Trust remains the property of the Trust. Users should not have an expectation of privacy in anything they create, store, send or receive on their computer. The Trust has the capability and right to monitor e-mails if there are suspicions of inappropriate use.

A disclaimer is to be added to every individual's e-mail as follows:

Legal disclaimer: *This email is confidential and intended solely for the use of the individual to whom it is addressed. Any views or opinions presented are solely those of the author and do not necessarily represent those of the Trust. If you are not the intended recipient, be advised that you have received this email in error and that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this email in error please notify the sender. This e-mail has been checked for viruses using anti-virus software*

The Trust e-mail system allows users to retain in their mailbox a maximum of xMb of mail and attachments. When this limit is reached the user will receive warnings that the box is over its limit and should archive any important mail to reduce the size of the mail box. Users are responsible for managing their own mailboxes and ensuring that messages which are no longer required are deleted. Users should be aware that sending large attachments affects the performance of the network and as such any attachments in excess of xMb should not be sent via e-mail.

To aid users a number of key do's and don'ts are set out below:-

DO	DON'T
▪ Think carefully when composing mails, the nature of e-mail is that it is often less formal than letters etc. This informality can cause differences in interpretation amongst recipients ▪ Use distribution lists appropriately. Is it important that all addressees receive this e-mail? ▪ Check your e-mails regularly, and respond to requests promptly. ▪ Advise people when you are not available by setting 'Out of office auto-reply' on the system. ▪ Be selective about who receives your e-mails, especially when using 'Reply to All'. Do all recipients need to see the reply? ▪ Remember that a mail from a Trust e-mail account reflects on the organisation. It is also admissible in a court of law and may require disclosure under the Freedom of Information Act ▪ Manage you mailbox ▪ Keep your password secure ▪ **Ask if you are in doubt**	▪ Send patient identifiable information by e-mail ▪ Send offensive, pornographic or illegal messages or material ▪ Use the e-mail accounts of others except where proxy rights have been granted ▪ Send global messages, except for alerts ▪ Send messages to those whom you are aware do not wish to receive the mail ▪ Use the account of another individual without official access to that account. ▪ Use the e-mail system for personal gain ▪ Forward junk mail, spam or chain mail. ▪ Send attachments in excess of 10Mb ▪ Open mail where you do not recognise the sender or the contents appears to be dubious – it may be a virus ▪ Open attachments with exe or vbs extensions ▪ Be caught put by the speed of e-mail. Think carefully, is your first reaction really the one that you want the recipient to receive

4.2.2 NHS Mail

The Trust, like all other NHS organisations, has subscribed to the NHS directory service. As part of this NHS mail accounts have been established for all staff.

NHS mail is a secure internet mail, calendar and directory service within which every employee has an “address for life” which is always @nhs.net and does not change as they move organisations. It is also available directly from the internet allowing users to access their mail from any location. This is in addition to the Trust account given to every user.

Unlike most e-mail systems NHSmail encrypts messages while in transit. The BMA has confirmed that it meets their requirements in respect of security and confidentiality and can be used to replace paper communication such as patient referrals and clinical enquiries.

However, NHSmail does not protect information before it has been sent or after it has been received. Therefore, users should only send clinical information if it part of an agreement between both parties which establishes the security requirements at both ends of the transmission.

The acceptable use policy for the use of the NHS mail and directory service is maintained by the NHS Information Authority. A copy of their policy is available form their web site (nww.nhsia.nhs.uk)

4.2.3 Internet Mail

Messages sent using commercial internet mail accounts (such as yahoo or hotmail) are particularly insecure and staff are advised not to use them for Trust business.

4.3 Personal Use

The Trust and NHSmail services systems are provided to users for businesses purposes, however the Trust wishes to encourage users to develop their IT skills and acknowledges that formal training is often best complemented by “trying things out” or personal use. Personal use, however, represents an area of concern not just in the NHS but in all sectors given the risks faced.

It is the Trust view that limited personal use is acceptable but such usage should not interfere with the performance of your job, therefore use of e-mail facilities for personal purposes should be confined to non working hours.

Further, such use should only be for personal purposes and should not be to support or pursue private businesses. Users should be particularly careful regarding the content of e-mails as such content such as jokes or images may be unacceptable where their nature is similar to the web site content described in Section 5 and Appendix A.

In particular users should ensure that:-

- Personal use is kept to a level that is not detrimental to the main purposes for which the accounts were provided;
- Priority is given to the use of accounts for business purposes;
- Personal use must not be for commercial purposes or any form of personal financial gain;
- Personal use must conflict with Trust policies and procedures; and,
- Personal use must not conflict with any of the users obligations as an employee of the Trust.

5. The Internet

5.1 Context

The internet is a valuable tool for research and dissemination of information. However, the risk associated with connection to and use of the internet are extreme and require significant management and control.

The Trust provides internet access to all staff through its connection to NHSnet which is a secured service, which aims to protect the NHS from many of the risk associated with the internet.

Users must not install or configure any connections to commercial internet service providers. Such connections are insecure and may, in certain circumstances, represent a breach of the Trust's Code of Connection to NHSnet which could result in the Trust being disconnected from NHSnet.

5.2 Business Use

Internet access is seen as a key facility in enabling users to perform their jobs. Access to web sites and service which are to support business (e.g. research) activities are deemed as acceptable.

5.3 Personal Use

Internet access is provided to users for businesses purposes, however Trust wishes to encourage users to develop their IT skills and acknowledges that formal training is often best complemented by "trying things out" or personal use.

It is the Trust's view that limited personal use is acceptable but such usage should not interfere with the performance of your job, therefore use of the internet for personal purposes should be confined to non working hours.

At all times there are a range of conditions that should be applied to such access viz:-

- Users must not access, download or transmit any obscene, indecent or pornographic images, data or other material;
- Users must not access, download or transmit any defamatory, sexist, racist or otherwise offensive images, data or other material;
- Users must not access, download or transmit any copyrighted material in a manner that violates that copyright;
- Users must not access, download or transmit any material that is designed or likely to annoy, harass, bully or inconvenience other people;
- Users must not access, download or transmit material created for the purpose of corrupting or destroying the data of other users;
- Users must not allow non-Trust persons access to systems;

- Use must be for personal purposes and not for the support of any private business ventures.

Such guidance does not represent the totality of possible inappropriate access. Users should be aware at all times that the principles of decency and legality will be applied. A simple rule of thumb could be described as "if the material could cause offence to even one individual then it is probably inappropriate"

The final "decision" on the appropriateness of material accessed will lie with the Trust. It is the Trust view that limited personal use is acceptable but this should be confined to non-business hours and should, at all times, be legal. Further, such use should only be for personal purposes. The use of Trust equipment to support or pursue private businesses is not acceptable.

5.4 Acceptable Types of Sites

Appendix A to this standard contains advice to staff on the suitability of certain types of sites / content. The list is not exhaustive and needs to be viewed on the basis of it being baseline guidance. The list is intended as relating to personal use rather than business use which, dependent on the nature of individual posts may require users to access some of the sites which are currently restricted or prohibited. If you require access to such sites in the course of your work you should advise the Head of IT in order that any confusion may be avoided.

For the purpose of this guidance the following categories of access are to be applied:-

Leisure Time	Access allowed outside of working hours.
Work Time	No access is allowed at any time of the day

6. Compliance

6.1 Responsibility

It is the responsibility of all users to ensure that they have read, understood and abide by this standard.

6.2 Review and Monitoring

The Trust has in place routines to regularly audit compliance with this and other standards.

In addition it reserves the right monitor usage and content where it suspects that there has been a breach of policy.

The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

In addition communications may be monitored (but not recorded) for the purpose of checking whether those communications are relevant to the purpose of the Trust's business, and the employees position with the Trust.

Any monitoring will be undertaken in accordance with The above act and the Human Rights Act.

6.3. Reporting Security Incidents

If any person becomes aware that there has been inappropriate use of equipment, e-mail or the internet they should report it to the Head of IT who will investigate the incident.

APPENDIX A – GUIDANCE ON ACCE PTABLE INTERNET SITES

CATEGORY	WORK TIME	LEISURE TIME
Violence / Profanity	Insert detail	
Partial Nudity		
Full Nudity		
Sexual Acts		
Gross Depictions		
Intolerance		
Satanic or Cult		
Drugs & Drug Culture		
Militant / Extremist		
Sex Education		
Questionable / Illegal / Gambling		
Alcohol &Tobacco		
Sports & Entertainment		
Search Engines		

Access to these types are sites are blocked / allowed by the Trust's internet filtering software.

This software also blocks the downloading of MP3 files.