

<u>Policy/Procedure Title</u>	Acceptable Use Policy		
<u>Sponsoring Director:</u>	Director of Finance & Information		
<u>Implementation Lead:</u>	Information Governance Manager		
<u>Impact:</u>	(a) <i>To patients</i>	None	
	(b) <i>To staff</i>	Yes	
	(c) <i>Financial</i>	None	
	(d) <i>Other</i>	None	
<u>Additional Costs:</u>	(a) <i>Training: N/A</i>	<i>Budget:</i>	
	(b) <i>Implementation: N/A</i>	<i>Budget</i>	
	(c) <i>Capital N/A</i>	<i>Budget</i>	
	(d) <i>Other N/A</i>	<i>Budget:</i>	
<u>Training implications:</u>			
<u>Date of consultation at:</u>	<i>Barnsley Information Governance Group – 27th January & 18th March 2009</i>		
<u>Alignment</u>			
<u>Date of Final Version:</u>	<i>18th March 2009</i>		
<u>Implementation Date:</u>	<i>April 2009</i>		
<u>Date of last review:</u>			
<u>Date of next review:</u>	<i>Annually or sooner if required</i>		
<u>Circulation Date:</u>	<i>April 2009</i>		
<u>Circulated Staff:</u>	<i>All Staff</i>	Yes	No
		Yes	

ACCEPTABLE USE POLICY

I INTRODUCTION

Electronic mail (E-Mail) and networks that support Internet Access are corporate assets and critical components of Barnsley NHS Foundation Trusts (BHNFT) communication systems. E-mail, internet and hospital system access is provided to aid staff in the performance of their duties. The efficient and acceptable use of these assets is essential to maintaining the Trusts business purposes. The purpose of this policy is to provide E-mail, Internet, Trust hospital systems and removable media users with guidance and direction on acceptable use.

1. POLICY STATEMENT

- 1.1** This policy applies to all employees of BHNFT and to any contractors who utilise E-mail, Internet and removable media.
- 1.2** It should be noted that this policy is not a definitive statement of the purposes for which the organisations facilities must not be used, all staff must conduct themselves at all times in a trustworthy and appropriate manner so as not to discredit or harm the organisation or its staff and in accordance with this policy.
- 1.3** Any breach of or refusal to comply with this policy is a disciplinary offence which may lead to disciplinary action in accordance with the organisations Disciplinary Policy, up to and including, in appropriate circumstances, dismissal without notice.

2. PURPOSE

- 2.1** The purpose of this policy is to ensure that all staff and contractors are aware of their individual responsibilities in relation to the use of e-mail, internet, removable media and hospital systems within BHNFT.
- 2.2** To identify the rules governing the use of E-mail, internet, removable media and hospital systems within BHNFT.

3. RESPONSIBILITIES

- 3.1** All employees and contractors of BHNFT are responsible for the compliance with this policy.
- 3.2** All employees are required to read and accept this policy on an annual basis.
- 3.3** Overall responsibility for the enforcement of this policy lies with the Chief Executive, or any individual identified by them as having responsibility in this area.

- 3.4 It is the responsibility of the delegated individual to implement the policy within the Trust and take appropriate action where misuse is covered.
- 3.5 It is the responsibility of the Information Governance department to maintain the policy in conjunction with the ICT department, reviewing it on an annual basis and following any major organisational changes to ensure its relevance.

4. DEFINITIONS

4.1 NHS Net Email

- 4.1.1 All Trust employees and contractors must comply with the NHS Mail Acceptable Use Policy at all times.
- 4.1.2 Any E-mails containing Person (staff and patient) Identifiable Data (PID) must only be sent via the NHS Mail facility. **No PID should be sent externally to organisations outside of the NHS Mail network without the use of encryption.**

4.2 Personal (internet web based) E-Mail

- 4.2.1 Many employees will have private external E-mail accounts that are provided by Internet Service Providers (ISP), which may be accessible via the Web, e.g. Hotmail accounts etc. **These accounts must under no circumstances be used to transfer PID or business confidential information. No E-mails containing such information are to be sent to or from these accounts.**

5. ACCESS

5.1 Internet, E-mail, hospital systems

- 5.1.1 Access to the Internet, E-mail and hospital systems will only be granted to users of the Trusts network following completion of the appropriate network access form (appendix 1) authorised by their line manager.
- 5.1.2 Staff will be required to attend training for any hospital systems before access will be granted.

6. ACCEPTABLE & UNACCEPTABLE USE

6.1 Acceptable Use – E-mail

- 6.1.1 The organisations E-mail system is considered a corporate resource and is to be used in connection with your work and the organisations business.
- 6.1.2 Email sent externally from the Trust must contain an appropriate legal disclaimer and statement of confidentiality.

6.1.3 Acceptable use of E-mail is based on common sense, common decency and civility and in accordance with UK legislation. E-mail must be used in the same way and with the same intent as any other form of communication.

6.1.4 It is the senders responsibility to ensure that confidential emails (whether business sensitive or staff/patient information) is sent via NHS Mail or with encryption protection.

6.1.5 Staff should note that it will not always be appropriate to communicate by email and individuals should always consider whether there is a more suitable method of communication, particularly, for example, in sensitive or highly confidential circumstances.

6.2 Unacceptable Use- E-Mail

6.2.1 The term 'unacceptable use' refers to any use which could lead to disciplinary action being taken against the individual user. Misuse of E-Mail will result in appropriate disciplinary action being taken.

6.2.2 The following constitutes as unauthorised access and may be subject to disciplinary action.

- Permitting anyone else to send E-Mail using the username or e-mail address you have been allocated

6.2.3 The use of organisational e-mail for private commercial activities. For example the buying or selling of goods or services (on-line shopping).

6.2.4 The use of e-mail for the purposes of gambling or the conducting of any illegal activities.

6.2.5 The use of e-mail for the forwarding of unsolicited mail or promotion of chain mail may result in disciplinary action being taken against the user. For example, the distribution of jokes, stories or images.

6.2.6 Any e-mail message that lays the sender or the organisation open to civil or criminal action.

- Libellous or defamatory material (defamation covers both words and images).
- Indecent or obscene material
- Abusing or menacing material that is likely to cause offence
- Material that is designed to likely to cause annoyance, inconvenience or needless anxiety.
- Material that harasses any other employee or third party, particularly on the basis of sex, ethnic origin, colour, nationality, religion, sexual orientation, marital status and disability.

- Material that infringes the copyright of another person or organisation
- Unsolicited commercial or advertising material

6.2.7 Web based e-mail accounts, for example Hotmail or other such accounts must not be used for business purposes.

6.2.8 The Trust reserves the right to monitor the use of E-mails via Human Resources and a request to NHS Mail.

6.3 Acceptable Use – Internet/Intranet

6.3.1 Access to the internet is provided for business use or for professional development and training, and can be used in relation to the professional activities of the authorised user and for the purpose of research and development. Limited use is permitted outside of work hours, subject to users not contravening the unacceptable use sections of this policy and consent from line management.

6.3.2 It is acceptable to save from the Internet where this does not contravene any of the unacceptable use activities listed below.

6.3.3 The downloading of software, including MP3 music files, video images, downloading of 'freeware' or 'shareware' software or evaluation software is not permissible.

6.4 Unacceptable Use – Internet/Intranet

6.4.1 Whilst limited use of the Internet for non-business related purposes is permitted, this use must not interfere with the performance of your duties, and must be conducted outside of your normal 'work' hours. For example, limited personal use will be permitted during lunch periods or prior to / following normal duty times, with the consent of the appropriate line manager.

6.4.2 Accessing or searching for sites, which display indecent, obscene, hateful, racist or otherwise objectionable material, is expressly forbidden. Access to these sites may contravene UK laws and may expose you as an individual and the Organisation(s) to criminal or civil liability. Users who persistently attempt to connect to unauthorised sites will have their Internet access terminated.

6.4.3 Any Intranet message board post that lays the sender or the organisation open to civil or criminal action.

- Libellous or defamatory material (defamation covers both words and images).
- Indecent or obscene material
- Abusing or menacing material that is likely to cause offence

- Material that is designed to likely to cause annoyance, inconvenience or needless anxiety.
- Material that harasses any other employee or third party, particularly on the basis of sex, ethnic origin, colour, nationality, religion, sexual orientation, marital status and disability.
- Material that infringes the copyright of another person or organisation
- Unsolicited commercial or advertising material

7 BLOCKING OF INAPPROPRIATE CONTENT

7.4 BHNFT will employ software to enable the blocking of sites, the content of which is deemed inappropriate.

7.5 Attempts to access web sites that display inappropriate content will be logged by the system and may result in disciplinary action being taken against the individual concerned up to and including dismissal without notice.

7.6 Attempts to access certain categories of site, specifically those which display or are connected to Child Pornography will result in immediate notification to Police. An attempt to access this kind of material is a criminal offence.

7.7 All use of Internet will be logged by the system, monitoring however is designed only to identify potential misuse of the organisations systems.

7.8 Where a user identifies a site that has been blocked that they require access to as part of their work, they can make a request to have the site opened for use.

7.9 Requests for a blocked site to be opened for use must be made using the form at Appendix 1.

7.10 Decisions as to whether a site will be unblocked for a particular user, or group of users or organisation wide will be made by the I.C.T Department. These decisions will be reviewed by the organisations Information Governance Lead to ensure appropriateness.

8 REMOVABLE MEDIA

8.4 Removable media for the purpose of this policy is defined as USB data/memory sticks, PDA's, CD Roms, floppy disks etc.

8.5 The use and transfer of un-encrypted removable media is strictly forbidden at the Trust.

8.6 Decisions as to who will be allocated encrypted removable media hardware will be made by the Information Governance Department.

8.7 Requests for encrypted removable media (USB data/memory sticks) can be made using the Trust's Case of Need form.

9 HOSPITAL SYSTEMS

9.4 Hospital systems for the purpose of this policy is defined as any system that contains Person Identifiable Data (PID) namely patient and staff information for eg PAS and ESR.

9.5 All use of hospital systems will be audited on a regular basis for accuracy and legitimate access relationship purposes.

9.6 All staff must have a legitimate reason to access any record on hospital systems and in manual format (health records). Any evidence of unauthorised access to a record will result in appropriate disciplinary action being taken, up to and including, in the appropriate circumstances, dismissal without notice.

9.4 The sharing of passwords for any hospital system is strictly forbidden at the Trust.

10 LEGAL REQUIREMENTS

10.4 The content of any E-mail sent either internally or externally to the organisation, or the content of any electronic information accessed or obtained from the Internet, must comply with UK law including the following legislation:

The Data Protection Act 1998
The Computer Misuse Act 1990
The Copyright Designs and Patents Act 1988
The Sex Discrimination Act
The Race Relations Act
The Laws of Libel
The Electronic Communications Act 2000
The Human Rights Act 2000
The obscene Publications Act
The Freedom of Information Act 2000

11 SECURITY

11.4 It is important that users maintain the security and confidentiality of the Organisations E-mail system. This may be achieved by:

- Not leaving yourself logged into the network / E-mail Systems / Hospital systems and not leaving your Computer unattended.
- Not allowing another person to use your E-mail account.

11.5 Users must not knowingly download a virus or malicious software.

12 MISUSE

12.4 Any mis-use of E-mail / Internet facilities will result in the user having access rights removed and will result in appropriate disciplinary action being taken, up to and including, in the appropriate circumstances, dismissal without notice.

12.5 Failure to comply with this and related policies will result in appropriate disciplinary action being taken, up to and including, in the appropriate circumstances, dismissal without notice.

12.6 Any use of the Internet / E-mail facilities for the conducting of illegal activities may be reported to the appropriate authorities and may result in an instant dismissal of the individual concerned.

13 MONITORING

13.4 Any monitoring of an E-mail / Internet use by the Organisation will be undertaken within the constraints of the Regulation of Investigatory Powers Act 2000 and the Lawful Business Practice Regulations, The Data Protection Act 1998 and the Human Rights Act 2000.

13.5 The lawful business practice regulations identify a number of purposes for which Organisations may monitor or record communications on their systems without the consent of the individual these are;

1. To establish the existence of facts relevant to the business, such as keeping records of communications where it is necessary or desirable to know the specific facts of the conversation.
2. To ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the business, such as monitoring to ensure that the Organisations E-mail/Intranet policy is being complied with.
3. To ascertain standards which ought to be achieved by persons using the system. Quality control or staff training.
4. To prevent or detect crime.
5. To investigate or detect the unauthorised use of the system.
6. To ensure effective operation of the system.

7. For the purpose of determining whether or not they are communications relevant to the business.

Where the Organisation intends to intercept communications without consent, the regulations require that all reasonable efforts are made to inform every person who may use the system that communications may be intercepted.

This Acceptable Use policy advises users that use of these systems is monitored, and by signing to accept the policy, users have consented to this monitoring taking place.