Policy Title and ID number	**GEN 6.41 Acceptable Use of ICT Systems (Assets) Policy**			
Sponsoring Director:	**Director of Quality & Standards**			
Implementation Lead:	Information Governance Manager			
Impact:	*(a) To patients*	None		
	(b) To Staff	Yes		
	(c) Financial	None		
	(d) Equality Impact Assessment (EIA)	Completed:		
	(e) Other	None		
Additional Costs:			*Budget Code*	*Revenue or Non Revenue*
	(a) Training:	*£0*		
	(b) Implementation:	*£0*		
	(c) Capital:	*£0*		
	(d) Other	*£0*		
Training implications:	*To be incorporated into induction:* **Yes**		*Other:*	
Date of consultation at:	*Board of Directors*		For note: January 2011	
	Executive Team		*23rd December 2010*	
	Divisional Medical Directors/Clinical Directors			
	Assistant Divisional Directors/Heads of Department			
	Non-Clinical Risk Committee		*7th December 2010*	
	Joint Partnership Forum		*14th December 2010*	
	Local Negotiating Committee		*N/A*	
	Infection Control Committee:		*N/A*	
	Health & Safety Committee		*N/A*	
	Information Governance Group		*28th October 2010*	
Alignment	*HR:*		Yes	
	Strategic Direction:			
	Board Assurance:			
	Clinical Governance:			
Date of Final Draft:	*October 2010*		Issue Number:	1.3
Date of Final Approval:			Approved by:	
Implementation Date:	*January 2011*			
Date of last review:	August 2011	Date of next review:	Aug 2012	
Circulation Date:	*September 2011*			
Circulation:			Yes	Comment
	Directors		Yes	
	Non Executive Directors		Yes	
	Divisional Medical Directors/Clinical Directors		Yes	
	Medical Staff Committee/SMSF		Yes	
	Assistant Divisional Directors		Yes	
	Assistant Nursing Directors		Yes	
	Heads of Department		Yes	
	H&S Committee Members		Yes	
	Policy database/warehouse		Yes	
	Others (to be listed):		All Trust Staff	Via Electronic Acceptance

Acceptable Use of ICT Systems (Assets) Policy

CONTENTS

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 users of Trust ICT Assets with guidance and direction on acceptable use.

1. POLICY STATEMENT

1.1 This policy applies to Trust employees, contractors, agency staff and individuals from external organisations who have been authorised access to Trust ICT Assets.

1.2 All staff will be required to sign and accept the terms of this policy electronically on an annual basis.

1.3 This policy should be read in conjunction with the Trust Safehaven and Disciplinary Policies.

1.4 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.

1.5 Any breach of or refusal to comply with this policy is a disciplinary offence which may lead to disciplinary action in accordance with the Trust 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 individuals who are authorised to access Trust ICT Assets are aware of their individual responsibilities.

2.2 To identify the rules governing the use of ICT Assets within the Trust.

3. RESPONSIBILITIES

3.1 All employees, contractors, agency staff and individuals from external organisations who have been authorised access to our ICT Assets are responsible for the compliance with this policy.

3.2 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.

3.3 It is the responsibility of the delegated individual to implement the policy within the Trust and take appropriate action where misuse is covered.

3.4 It is the responsibility of the Information Governance department to maintain the policy in conjunction with the Human Resources and ICT department, reviewing it on an annual basis and following any major organisational changes to ensure its relevance.

4. DEFINITIONS

4.1. ICT Asset

ICT Asset defines any hospital IT system in use at the Trust e.g. Email, Internet, Clinical Systems.

4.2. Corporate Email Systems

The organisations corporate E-mail system is NHS Mail.

4.3. Personal Email Systems

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, Gmail and Yahoo accounts.

4.4. Acceptable Use

The term ‘acceptable use’ is based on common sense, common decency and civility and in accordance with UK legislation.

4.5. Unacceptable Use

The term ‘unacceptable use’ refers to any use which could lead to disciplinary action being taken against the individual user.

4.6. Removable Media

Removable media for the purpose of this policy is defined as removable storage devices used to transport or store information eg. USB data/memory sticks, PDA’s, CD Roms.

5. ACCESS AND MONITORING

5.1. Access to ICT Assets will be granted to those with a legitimate need by the relevant Information Asset Administrator (IAA) following completion of the password form which has been authorised by their line manager (Appendix A).

5.2. Staff will be required to attend training for ICT Assets before access will be granted.

5.3. All use of ICT Assets will be logged. Monitoring however, is designed only to identify potential misuse, accuracy issues and legitimate access relationships of the organisations assets.

5.4. The sharing of passwords and/or smartcards for any ICT Asset is strictly forbidden.

5.5. All staff must ensure that all workstations are locked, logged off, smartcards removed to maintain the security and confidentiality of Trust ICT Assets and service user details.

5.6. All staff must have a legitimate reason to access any record on ICT Assets. Any evidence of unauthorised access to a record will result in appropriate disciplinary action being taken.

5.7. 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.

5.8. 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.

6. EMAIL

6.1. All staff working for or on behalf of the Trust will have access to the Corporate Email System.

6.2. All authorised users of the Corporate Email system must comply with the Connecting for Health NHS Mail Acceptable Use Policy at all times.

6.3. The organisations Corporate Email system is considered a corporate resource and is to be used in connection with your work and the organisations business only.

6.4. Emails containing Person (staff and patient) Identifiable Data (PID) and business sensitive information must only be sent to individuals with a legitimate need via the secure the Corporate Email system, a list of approved email addresses can be found in Appendix B.

6.5. Emails and documents that require transferring outside the secure Corporate Email system must be encrypted to the required level (advice can be sought from the Information Governance Department on how to do this).

6.6. 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.

6.7. Email sent externally from the Trust must contain an appropriate legal disclaimer and statement of confidentiality.

6.8. Acceptable Use of Email

6.8.1. E-mail must be used in the same way and with the same intent as any other form of communication.

6.8.2. 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.

6.8.3. The use of personal email systems is permitted for personal use.

6.9. Unacceptable Use of Email

6.9.1. 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

6.9.2. The use of personal email systems for Trust/business purposes.

6.9.3. The use of the Corporate Email system for private or commercial activities. For example the buying or selling of goods or services (on-line shopping).

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

6.9.5. 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.

6.9.6. Any e-mail message that lays the sender or the organisation open to disciplinary, civil or criminal action, including but not limited to:

- 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. INTERNET & INTRANET

7.1. The Trust employs software to enable the blocking of sites, where the content of which is deemed inappropriate.

7.2. 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.

7.3. 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.

7.4. 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 to the ICT Department.

7.5. 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

7.6. Acceptable Use Internet/intranet

7.6.1. 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.

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

7.7. Unacceptable Use – Internet/Intranet

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

7.7.2. 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.

7.7.3. 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.

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

7.7.5. Any Intranet message board post that lays an individual or the organisation open to disciplinary, civil or criminal action, including but not limited to:

- 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

Please see a list of do's and don'ts in Appendix D.

7.8. Social Media

7.8.1 The Trust recognises that social networking sites are increasingly useful communication tools and acknowledge the right of staff to freedom of expression. However, staff must be aware of the potential legal implications of material which could be considered confidential, abusive or defamatory.

7.8.2 Staff should be aware that the Trust reserves the right to use legitimate means to scan the web, including social networking sites for content that it finds inappropriate.

7.8.3 The Trust may take disciplinary action if necessary against any employee who brings the organisation into disrepute by inappropriate comments on social networking sites or personal internet sites.

For further information on Social Media please refer to Appendix E.

8. REMOVABLE MEDIA

8.1. The use and transfer of un-encrypted removable media is strictly forbidden at the Trust.
8.2. Removable media devices are requested through the Trust Case of Need form authorised by the requestor's line manager.

9. MISUSE

Failure to comply with this and associated policies, along with any misuse of IT Assets will result in the user having their access rights postponed/removed pending an investigation and could result in appropriate disciplinary action.

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 summary dismissal of the individual concerned.

10. LEGAL REQUIREMENTS

The content of any information/data 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

This Acceptable Use Policy should be read in conjunction with the Trusts Mobile Phone Policy.

APPENDIX A

Password Form to be added when reviewed

APPENDIX B

Approved Email Addresses: Extract from NHS Mail AUP Section 4.1

4.1. The NHSmail service is a secure service, this means that NHSmail is authorised for sending sensitive information, such as clinical data, between NHSmail addresses (i.e. from an '@nhs.net' account to an '@nhs.net' account), Government secure email domains (between *.nhs.net and *.gsi.gov.uk *.gse.gov.uk *.gsx.gov.uk), Police National Network/Criminal Justice Services secure email domains (between *.nhs.net and *.police.uk *.pnn.police.uk *.scn.gov.uk *.cjsm.net), Ministry of Defence secure email domains (*.nhs.net and *.mod.uk) and Local Government/Social Services secure email domains (*.nhs.net and *.gcsx.gov.uk). If you intend to use the service to exchange sensitive information you should adhere to the following guidelines:

4.1.1. You should make sure that any exchange of sensitive information is part of an agreed process. This means that both those sending and receiving the information know what is to be sent, what it is for and have agreed how the information will be treated

4.1.2. Caldicott principles should apply whenever sensitive information is exchanged

4.1.3. As with printed information, care should be taken that sensitive information is not left anywhere that it can be accessed by other people, e.g. on a public computer without password protection

4.1.4. When you are sending sensitive information you should always request a delivery and read receipt so that you can be sure the information has been received safely. This is especially important for time-sensitive information such as referrals

4.1.5. You must not hold patient identifiable data in your calendar if your calendar may be accessed by other people who are not involved in the care of that patient

4.1.6. If patient identifiable information is visible to other people it is your responsibility to make sure that those people have a valid relationship with the patient

4.1.7. You must always be sure that you have the correct contact details for the person (or group) that you are sending the information to. This is especially important if you are sending information using the fax or SMS services. If in doubt you should check the contact details in the NHS Directory

4.1.8. You may only use the NHSmail service for patient referrals if Choose and Book has not yet been implemented in your organisation; the Choose and Book service is unavailable to you for some reason, or the service you need to refer to is not available via Choose and Book

4.1.9. If it is likely that you may be sent patient and/or sensitive information you must make sure that the data is protected. You should only access your account from secure, encrypted devices which are password protected and unattended devices must be locked to ensure that data is protected in the event of the device being lost or stolen

APPENDIX C

Sales and Swaps

This message board provides a facility for Barnsley Hospital staff to part with, and acquire, goods in a safe manner. The use of the system will be managed, and posts will be checked to ensure proper and ethical use of the board.

Please note: Barnsley Hospital NHS Foundation Trust does not endorse any goods or services advertised on this site. You enter into any contracts for sale of goods or services at your own risk. This Board is provided for the benefit of Trust employees, and any misuse of the Board will result in the user account being de-activated.

The rules...

Do

1. Place a sale or want ad
2. Respond to ads politely
3. Feel free to recommend services
4. Feel free to advertise property to rent

Don't

1. Aggressively sell goods or services or use bullying tactics
2. Repeat advertise goods or services more than once a month
3. Use vocabulary or humour that could be classed as inappropriate or offensive
4. Advertise goods or services that will break any UK/EU laws
5. Advertise anything that might bring the Trust's reputation into disrepute

Finally, advertisements are to contain no reference to any endorsement by Barnsley Hospital

Note: Any contravention of the "Don'ts" will result in the post being removed, and your account either suspended or de-activated.

Appendix D
Caldicott Principles

The Caldicott Standards are based on the Data Protection Act 1998 principles and again are set out in the form of Principles

The Caldicott Guardian for the Trust is the Medical Director.

Principle 1: **Justify the Purpose**
Every proposed use or transfer of patient-identifiable Information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate Guardian.

Principle 2: **Don't use Patient-Identifiable Information unless it is absolutely necessary**
Patient-identifiable information items should not be used unless there is no alternative

Principle 3: **Use the minimum necessary Patient-Identifiable Information**
Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability

Principle 4: **Access to Patient-Identifiable Information should be on a strict need-to-know basis**
Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see

Principle 5: **Everyone should be aware of their responsibilities**
Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are aware of their responsibilities and obligations to respect patient confidentiality

Principle 6: **Understand and Comply with the Law**
Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements

Appendix E

'Social media' is the term commonly given to websites and online tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests. As the name implies, social media involves the building of communities or networks, encouraging participation and engagement.

The main types of social media are networking services which contain category places (such as former school year or classmates), means to connect with friends (usually with self-description pages) and a recommendation system linked to trust. Popular methods now combine many of these, with Facebook and Twitter widely used worldwide.

Personal use of social media – personal responsibilities

Barnsley Hospital NHS Foundation Trust (the Trust) recognises that whether or not you as an individual choose to create or participate in an online social network or any other form of online publishing or discussion is your own business. The views and opinions you express are your own.

As an employee of the Trust it is important to be aware that posting information or views about the Trust can not be isolated from your working life. Any information published online can, if unprotected, be accessed around the world within seconds and will be available for all to see.

When using social media in your personal lives please consider the following:

- You are **personally responsible** for any content you publish.
- All Trust employees are reminded that we need to maintain both patient and
- colleague confidentiality as outlined in **Confidentiality Code of Conduct** and the **Information Governance Policy**
- Do not let your use of social media interfere with your job and always access in your own time. See the **Acceptable Use of IT Systems (Asset) Policy**

You should be aware that information posted online is subject to precisely the same laws of defamation and libel as that which is published in hard copy. Therefore, you can be sued for libel for any defamatory statements you post about other individuals or organisations. You should be aware that this is a personal liability.

Personal use of social media – professional responsibilities

If you are using social media and identify yourself as a Trust staff member use the following guidelines:

1. Do not reveal confidential information about our patients, staff, or the Trust

2. Do not engage in activities on the intranet which may bring the Trust into disrepute
3. Do not use the internet in any way to attack or abuse colleagues
4. Do not post defamatory, derogatory or offensive comments on the internet about colleagues, patients, your work or the Trust.

Failing to meet the guidelines above may be treated as gross misconduct and would be dealt with under the Trust's disciplinary process.

Why do we need social media guidance?

Below are some examples of why there is a need to be careful when using social media:

- 'Checking in' to Barnsley Hospital via facebook when beginning work and heavily interacting on facebook throughout the day.
  WHY?
  - It may appear that you are not busy in your job. Think how this may look to the public or your work colleagues.

- Posting or being 'tagged' in inappropriate images on social network sites (such as facebook, flickr, twitpic).
  WHY?
  - Photos can sometime bring individuals professionalism into question.
  - Seven doctors and nurses were suspended from a hospital in Swindon 2 years ago while participating in the 'planking' phenomenon for breaking a number of hospital regulations.
    See:http://www.timesonline.co.uk/tol/life_and_style/health/article6827618.ece

- Tweeting, blogging or posting about a patients experience or treatment that you have experienced or witnessed that day.
  WHY?
  - You could be breaching patient confidentiality.
  - No matter how private you think the forum is in which you are sharing your comments there is potential for the wrong people to see it: http://www.mirror.co.uk/news/top-stories/2009/01/11/exclusive-marks-spencer-staff-ridicule-customers-on-facebook-115875-21033664/

When to contact the communications team
Contact the Trust's Communications Team:

- If you are contacted by a journalist or someone from the media about your online publications that relate to the Trust. You should seek advice from your line manager and the Communications Team before responding.

- If you become aware of breaches to the guidelines that may bring the Trust or staff into disrepute.

Ask yourself the following question before you post – will it affect the Trust, patients, staff or perceptions of the public? If the answer is yes then you might want to think again!

Acknowledgements

- Norfolk and Norwich University Hospitals Policy on the personal use by staff of social media 2009
- Devon County Council social media and online participation policy and guidelines 2010
- North Yorkshire and York PCT E-mail and Internet Policy 2009

Web Site Un-Blocking Request Form

You are required to complete this form and return to IT Support Services to request access to web sites (URL's - Uniform Resource Locators) that are blocked by the Trust's Internet content filtering software.

I require access to the following website(s):-

Website Address (URL)	Reason for Access

Staff Name: (Block Capitals) .....

Department: .....

Staff Signature: ..... Date:.....

To be completed by the Applicants Manager

I approve this request for access to the listed website(s).

Manager Name (Block Capitals) .....

Manager Signature: .....

Date: .....

To be completed by the ICT Department

Access Approved/Denied:..... Signature : .....

Date: ..... Reason for Non-Approval: .....

.....

.....

.....