This policy is applicable to services provided by Heartlands, Good Hope and Solihull Hospitals Divisions.

ICT Acceptable Use Policy

Key Points

- To ensure that staff that have access to and use IT services and information assets are aware of and understand their responsibilities for the safe and professional use of ICT

Key Changes

- This is a new policy and replaces any previous guidance or policy that may be in place

Paper Copies of this Document

- If you are reading a printed copy of this document you should check the Trust's Policy website (**http://sharepoint/policies**) to ensure that you are using the most current version.

Ratified Date: 18th April 2016
Ratified By: Chief Executives Group
Review Date: April 2018
Accountable Directorate: ICT
Corresponding Author: Information Systems Security Specialist

Meta Data

Document Title:	ICT Acceptable Use Policy
Status	Final: v1.0
Document Author:	Information Systems Security Specialist
Source Directorate:	ICT
Date Of Release:	20th May 2016
Ratification Date	18th April 2016
Ratified by:	Chief Executives Group
Review Date:	April 2018
Related documents	Information Security Strategy Confidentiality policy Data Protection Policy Safe Haven Policy and Procedure Mobile Computing policy Photographic Video and Mobile Device Consent and Confidentiality Policy Policy and Procedure for Social Media and online participation Records Management Policy Retention, Disposal and Destruction of Records policy Disciplinary Policy and Procedure Network and IT Security Policy ICT Administrators Code of Conduct Information Risk Management Policy Being Open Policy
Superseded documents	Email Policy Internet Policy
Relevant External Standards/ Legislation	Data Protection Act 1998 Freedom of Information Act 2000 Computer Misuse Act 1990 Criminal Justice Act 1988 Copyright, Designs and Patents Act 1998 Caldicott Principles Obscene Publications Act 1959 Equality Act 2010 Regulation of Investigatory Powers Act 2000

	Sex Discrimination Act 1975 Privacy and Electronic Communications Regulations 2000 Protection of Childrens Act 1978 Defamation Act 1996 Statutory Duty of Candour HSCIC Infrastructure Security Good Practice Guidelines Information Security Management: NHS Code of Practice Computer Misuse Act 1990 ISO27001 Communications- Electronics Security Group (CESG) Guidance ICO Employment Practices Code
Key Words	Email, Internet, confidentiality, unauthorised access, software, viruses, personal use, monitoring

Revision History

Version	Status	Date	Consultee	Comments	Action from Comment
0.1	Draft	20/2/2015	Information Systems Security Specialist	Initial draft	
0.2	Draft	22/12/15	Information Systems Security Specialist	Further development of content	Content updated
0.3	Draft	07/01/16	Head of ICT Business Development	Minor comments	Content updated
0.4	Draft	11/01/16	IG Committee, ICT Senior Leads, Key IT staff	Amendments to formatting and content.	Policy updated. Removed section 6.15 Clear Screen as covered in Section 6 and in Trust Network and IT Security Policy.
0.5	Draft	02/02/16	Trust Convenor	Add reference to Being Open Policy/ Duty of Candour and implications of breach including ICO action/ fines	Content updated and references added.

1.0	Final	05/02/16	IG Committee, Policy Group, JNCC	Expand section on monitoring and compliance to reflect that IG committee receive reports on policy effectiveness, and any breaches will be investigated through appropriate HR policies.	Updated. Policy approved by JNCC.
1.0	Final	18/04/2016	Chief Executives Group	Policy approved	

Contents

1 Circulation

This policy applies to all staff, contractors and any other person who works for, or with the Heart of England NHS Foundation Trust (herein known as the Trust) and has access to IT services and information assets.

2 Scope

This policy applies to the use of all IT services and information assets including (but not limited to) email, internet, clinical and corporate systems, mobile devices and social media by all staff employees of the Trust, non-executive Directors, contracted third parties (including agency staff), students/trainees, bank staff, staff on secondment and other staff on placement with the Trust that have access to Trust IT and information assets.

The policy also applies to IT assets managed or hosted by third parties of behalf of Heart of England NHS Foundation Trust.

Includes: This policy includes (but is not limited to) email, internet, clinical and corporate systems, network usage, mobile devices (as defined in the Trust Mobile Computing policy) and social media (as defined in the Trust Policy and Procedure for Social media and online participation).

3 Definitions

Confidentiality
Ensuring that personal, sensitive and/or business confidential information is protected from unauthorised access and is accessible only to those with a legitimate right to access.

Integrity
Ensuring that information can be relied upon to be accurate.

Availability
Ensuring that information is available to those that need it, when they need it.

Personal Confidential Information
Personal information about identified or identifiable individuals both living and deceased, which has been given in confidence or is owed a duty of confidence and should be kept private or secret.

IT Service
Trust wide service and communications facilities provided by ICT for business purposes, for example hardware and software components of the ICT infrastructure, file storage, email, internet, messaging services, networks (including wi-fi).

Information asset
An information asset is an identifiable and definable asset owned or contracted by an organisation which is 'valuable' to the business of that organisation.

Intellectual property
Intellectual property is something unique that has been created; intellectual property rights apply to exclusive rights to assets to which intellectual property applies. Anything that has been created by an individual as part of their employment will usually remain the property of the organisation that employed them.

Unauthorised access
Unauthorised access applies when an individual gains or attempts to gain access to information or IT services that they are not authorised to access.

Malware
Short for 'malicious software*',* malware is the term used to describe software used to disrupt computer operation, gather sensitive information, or gain unauthorised access to computer systems. Malware includes computer viruses, spyware and other malicious programs.

SPAM
SPAM is the terminology usually given to irrelevant or unsolicited messages sent typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc.

Social Media
Social media refers to the websites and applications that enable users to create and share content or to participate in social networking.

Social Networking
Social networking is the social interaction among people in which they create, share or exchange information and ideas in virtual (online) communities and networks. Popular examples of social networking are Facebook and LinkedIn.

Payment Card Industry Data Security Standards (PCI DSS)
PCI DSS is the Payment Card Industry Data Security Standard; is a worldwide standard set up to help businesses process card payments securely and reduce card fraud. It applies strict standards and controls for organisations that process of cardholder data to protect sensitive cardholder data.

4 Reason for development

The Trust expects its IT services and assets to be used in a professional manner that does not compromise the Trust, the NHS or its employees in any way.

All staff, contractors and other persons that have access to IT services and information assets are granted access to these systems and information held within them because it is considered essential to their role; however the inappropriate use of IT systems and information assets can expose the Trust and individuals to technical, professional and legal risks.

This policy describes the responsibilities and acceptable use of IT and information assets by setting out the principles and standards that apply to all staff, contractors and any other person who works for, or with the Trust or NHS and has access to Trust IT services and information assets.

Within this policy these people are referred to as ‘users’

This policy should be read in conjunction with the Trust’s Information Governance, ICT and HR Policies and the Trust Policy and Procedure for Social Media and online participation.

5 Aims and Objectives

The policy has been developed to:

- Ensure that users are aware of their responsibilities when accessing and using IT services and information assets and understand the associated legal and technical risks.
- Ensure legal and statutory requirements are met
- Minimise the risk of inadvertent, accidental or deliberate unauthorised access or disclosure of information
- Outline the consequences of a breach of this policy for the Trust and the individual

Failure to comply with the policy may result in formal disciplinary action or other action being taken against individuals by the Trust.

Furthermore failure to comply may lead to civil or criminal action by external regulatory bodies such as the Information Commissioner’s Office, who have the power to impose financial and criminal sanctions against individuals and the Trust.

6 Standards

6.1 General Security

The following security controls must be applied by users to safeguard IT services and information assets.

- Always position your screen away from visitors and general public
- The Trust operates a Clear Screen Policy. Always lock your screen when away from your desk
    - For Windows devices use Crtl-Alt-Del and Lock this computer or Windows L
    - For Mac devices use Ctrl-Shift-Eject, or Ctrl-Shift-Fn-Power
- Password protected screen savers should be activated when a computer is left unattended, or not accessed for a period of time.
- Never loan your Smartcard to another person or disclose your PIN
- Always remove your Smartcard from the reader when not in use and keep it securely on your person
- Never leave portable equipment unattended, lock away when not in use
- All Trust information, in particular confidential and person identifiable information, should be stored on network drives or within the appropriate clinical or corporate systems and not on local hard drives (C drive).
- When emailing personal confidential information the secure methods detailed in Appendix 1 must be applied.
- Only Trust approved encrypted USB memory sticks can be used to store Trust data Contact the ICT Service Desk if you are unsure whether a device you are using is Trist approved.
- Where a system presents a ‘break glass’ prompt which asks you to record your reason for accessing information or systems, a valid reason for access must be recorded, for example an incident/ complaint/ support reference number to support why access is required. The reason for access must be traceable to evidence that access is legitimate and necessary.
- Never load unauthorised software to your computer without first checking with IT
- Notify the ICT Service Desk of any leavers or changes to staff roles so that access can be terminated or amended

- Only authorised Trust staff and third parties are permitted to move any HEFT ICT equipment, whether within an office or to another site, unless specifically approved by the Head of Technical Services or Information Systems Security Specialist.
- Payment card information must not be processed on the Trust IT network, as the Trust does not hold the required accreditation (PCI DSS) to process this type of data. Any processing of payment card information must be via a PCI-DSS compliant service provider or payment gateway service (such as Mastercard, Worldpay, TNSPay).
- Any breaches or risks relating to the security of information and IT assets must be reported using the Trust Incident Reporting and Management Policy and Procedure.

Users should be aware that IT systems will be monitored using audit trails and log files to ensure appropriate use, any misuse will be subject to investigation and may lead to disciplinary action, termination of contract and/ or criminal proceedings.

6.2 Username and Passwords

6.2.1 Individual accounts

Users are personally responsible for the security of their individual login details and will be held responsible for any activity carried out using their login details or Smartcard.

Smartcards, passwords, PIN numbers and access codes must not be shared with anyone.

Password must not be written down and left visible to others, or kept with mobile devices e.g. Laptops, iPads

Passwords must be hard to guess and contain at least six characters, The minimum password requirement is that It must include three or the four following types of character:

- Number
- Lower case letter
- Upper case letter
- Special character such as !#£$

Passwords should be changed at regular intervals; system should be configured to automatically force regular password changes and to prevent reuse of passwords.

Users are held accountable for all activity undertaken using their account. If you suspect that someone else may know your password you must change it immediately

using the change password function, if available, or by contacting the IT Service Desk or appropriate system administrator.

If you anticipate that someone else needs access to data held within your account you must arrange for data to be transferred in advance.

Managers must ensure that when a person leaves the organisation a handover of Trust takes place in advance of the leave date and Trust data held in individual file storage areas (home drives), email accounts etc is transferred to the appropriate colleague to ensure service continuity.

6.2.2 Generic accounts

Generic accounts are not recommended. In exceptional circumstances, where an individual named account cannot be used for the intended purpose, generic accounts may be approved.

Where this is the case the generic account must have a nominated owner that takes responsibility for the security of the account and ensures that all users of the account are aware of and comply with the relevant Trust policies, including the ICT Acceptable Use policy.

Passwords will not be issued for generic email accounts. Users individual email accounts will be configured to enable delegated access to the generic email account.

6.3 Confidentiality

Some users will, through their access to Trust systems, have visibility of personal confidential information relating to the Trust, patients, employees and corporate confidential information. This information must be kept strictly confidential at all times and must be managed in line with the Data Protection Act 1998, NHS Guidance and Trust Policies on Confidentiality & Data Protection, Information Security, Information Governance and other related policies.

Users must apply the appropriate security procedures that are currently in place (as outlined in the Confidentiality and Data Protection; and the Information Security Policies) or that may be introduced by the Trust.

Users must not access any healthcare or personal information relating to themselves, their family, friends or acquaintances, unless directly involved in the individuals clinical care.

When transferring personal confidential information, the Trust Safe Haven Policy and Procedures must be followed. The secure methods for emailing confidential information are detailed in Appendix 1.

Postings placed on the Internet must reflect the standards and policies of the Trust.

Under no circumstances should any information of a **confidential** or **sensitive** nature be placed on the internet.

6.4 Data Protection

The Trust is registered as a data controller under the Data Protection Act 1998 and is committed to fulfilling its obligations in respect of personal data it holds about individuals and patients.

All patient and personal data provided to the Trust will be treated as confidential and not be used other than for legitimate purposes. Users must ensure that they are trained and comply with the provisions of the Data Protection Act 1998 in relation to any patient and personal information they handle as part of their role.

Refer to the Trust's policies relating to Information Governance, Confidentiality and Data Protection.

6.5 Defamation

The laws applying to electronic communication are the same as for any other written communication. Sending an email is effective as sending a letter on Trust headed paper. By posting to the Internet or by storing, sending or circulating any material by e-mail that contains inaccurate or libellous comments about people or organisations users may be exposing both themselves and the Trust to the prospect of legal action.

6.6 Formation of Contracts

The Trust must not be committed to any form of contract through the exchange of email messages or through the Internet. E-mail is just as capable of forming or varying a contract as a letter. The Trust must not be committed to any obligations via e-mail unless appropriate authority has been given.

Subscriptions to news groups and mailing lists using Trust email should be for a work-related purpose only.

6.7 Disclaimers

A disclaimer will automatically be attached to all outgoing email. Users should not create their own 'version' as part of an e-mail 'footer'. This is designed to limit the Trust's potential liability with regard to contents of e-mail.

6.8 Copyright and Intellectual Property Rights

Most information and software is subject to copyright or other intellectual property rights protection. Trust systems must not be used to store, send, receive or view any material that there is reason to suspect may be in breach of copyright.

There are serious implications for both the Trust and the INDIVIDUAL if an organisation is found to be in breach of legislation relating to copyright.

Any processes, data or systems development carried out as part of your role with the Trust will remain the intellectual property of the Trust unless a prior legal agreement is in place.

For further information please refer to the Copyright Licensing Agency website: www.cla.co.uk.

6.9 Software

Only licensed and approved software may be used on Trust systems. The use of, or copying of software is subject to licensing and copyright restrictions and is not permitted unless it is within the remit of the licence agreement.

There are serious implications for both the Trust and individuals if an organisation is found to be using illegal copies of software, or are inadequately licensed. The copying of Trust software for personal use is not permitted.

The Trust will treat any unauthorised use, or copying of software as a serious breach of policy.

Software downloaded from the Internet must not be installed on Trust systems without written authorisation from the ICT department.

6.10 Malware, viruses and SPAM

All IT equipment that has connectivity to the Trust network MUST have up to date virus protection software installed, and must be updated with relevant software patches. CDs or removable media from untrusted sources may contain viruses and should not be used on Trust systems.

E-mails may contain viruses or malicious code that can cause disruption to the Trust's IT systems.

Any e-mails and attachments that have been received from unknown or untrusted sources should not be opened, but should be reported to the appropriate IT Service Desk, as should excessive quantities of unsolicited e-mail and junk mail / SPAM.

Knowingly distributing a virus or malicious code, or failing to act responsibly to protect Trust systems from disruption will be considered a breach of this policy.

6.11 Personal Use

Information systems are provided for Trust use, however, limited personal use of the Trust e-mail system and Internet is acceptable providing that all of the following conditions are met:

- It should be outside of working hours or during breaks.
- It should not interfere with work performance.
- It must not be used for personal profit (e.g. running a business) nor for the benefit of any non NHS organisation
- It must comply with the provisions of this policy.

Personal use will be subject to the same monitoring as business use, as defined in Section 9 of this policy.

The e-mail system should not be used for forwarding chain letters received.

Data for personal use should not be stored on Trust systems. This applies particularly to image, video and music files and to software.

Abuses of this privilege are regarded as misuse of Trust equipment and may lead to removal of system access and/or further action.

6.12 Social Networking & Blogging

The term Social Networking is used to cover such internet sites as Facebook, LinkedIn. It also includes blog sites, internet homepages and other user interactive services.

These media provide a number of benefits in which Trust staff may wish to participate in their personal life; however staff are reminded of the Trust policy on personal use of the internet when accessing such sites from the workplace and that activity may be monitored as detailed in section 9.0 of this policy.

The following principles also apply when using social media:

- Staff must not upload or post confidential or personal information of patients and/or their relatives, colleagues, or the Trust.
- Staff must not upload or post photographs of another Trust employee taken in the work situation or in their working uniform.
- Staff must not upload or post defamatory, derogatory or offensive statements about colleagues, patients, their work or the Trust.
- Staff must not engage in activities on the Internet which might bring the Trust into disrepute.
- Staff must not use their Trust or NHS details, including postal address or email address when subscribing to internet services for personal use
- Staff must not use social networks or the internet to monitor or befriend patients

Refer to the Trust policy on social media and online participation for further information.

Any request to engage in online activities associated with work for the Trust should be subject to information risk assessment and approved by the Head of Communications and/ or relevant Information Asset Owner.

6.13 Unacceptable Use

Some activity is completely unacceptable, and will lead to further action.

Trust IT systems must not be used to create, store, exchange, view, download or post any material or references that are:

Obscene, sexually explicit, pornographic, racist, sexist, defamatory, libellous, or hateful.

AND / OR
Incite or depict violence, or describe techniques for criminal or terrorist acts

AND / OR

Breach any applicable law (e.g. Data Protection, Obscene Publications) or the Trust's Equal Opportunities, Harassment or related policies.

System users should not send an e-mail in any other person's name, nor allow any other person to use their e-mail account.

Users must not amend messages received and represent the content as original.

System users must not access or modify data or systems that they do not have authority to access. This not only breaches Trust policy, but also represents a breach of the Computer Misuse Act 1990.

In addition unacceptable use also covers engaging in computer hacking and other related activities, or attempting to disable or compromise the security of information contained in Trust systems.

The above list is not exhaustive but indicative of the type of usage/ access that is not permitted. Any violation of this could constitute gross misconduct under the Trusts disciplinary procedure and result in sanctions up to and including dismissal.

The Trust reserves the right to ban access to certain organisations and websites. Users should be aware that whilst the Trust may use automated content filtering to restrict access to certain sites, you should not assume that being able to access a particular website means that it is permitted.

6.14 Network and System Use

Before a new user can be allocated an account they must have understood and agreed to the terms of this policy.

There are strict security requirements for Trust networks that are connected to the national NHS (N3) network by way of mandated compliance with the Information Governance Assurance statement,

Users with access to the Trust network must not attempt, or deliberately assist others to attempt:

- Unauthorised access to hardware

- Unauthorised introduction of software or hardware components to the network
- Unauthorised modification of network components
- Unauthorised access to the Trust networks from other networks.
- Unauthorised circumvention of security features such as firewalls, passwords etc
- Unauthorised copying or distribution of software, documentation, or media associated with the Trusts IT systems
- Unauthorised removal or relocation of hardware, software, documentation or media associated with the Trusts IT systems

6.15 Housekeeping and Good Practice

Users must store their work in the most appropriate place (for example in network folder and in clinical or corporate systems) giving consideration to confidentiality and availability

Documents must not be stored locally (eg. on c drive) on a desktop computer, as they are not backed up and information may be irretrievable if the device fails or is stolen.

Documents stored in network file shares (eg. H drive) are stored in a secure area and backed up regularly by the ICT department.

Folders on network drives can be restricted to specific staff members, It is advised to store information on departmental shared drives and have the access restricted to authorised users only.

Obsolete files must be deleted regularly in line with the Trusts Records Management policies and the NHS Records Management: Code of Practice.

7 Responsibilities

7.1 Individual Responsibilities

Users
All users must:

- Be aware of and comply with the contents and implications of this and related policies in relation to the use of IT services and information assets
- Report any suspected or actual breaches of this policy using the Trust's Incident Reporting and Management Policy and Procedure.

Managers
Line managers are responsible for:

- Ensuring that all users under their management who have access to Trust IT services and information assets are aware of, and comply with, this and associated policies and procedures;
- Notifying HR of any suspected breaches of this policy so that appropriate action can be taken in accordance with the Trust Disciplinary policy. .

Information Asset Owners
Information Asset Owners must:

- Ensure that all users that have access to their information assets are appropriately trained and understand the requirements of this policy.
- Have procedures in place to undertake audits and monitor the appropriate use of information assets that they own.

7.2 Board and Committee Responsibilities

The Trust Board is responsible for ensuring that appropriate systems are in place to enable the organisation to deliver its objectives in relation to this policy. It will delegate responsibility for the ratification and delivery of the policy to the Information Governance Committee.

8 Training Requirements

All users and staff should be made aware of this policy and their responsibilities, and be appropriately trained in the use of IT services and information assets. This should include their responsibility for the appropriate use of IT services and information assets and their obligation to comply with relevant policies and procedures.

9 Monitoring and Compliance

The Trust reserves the right to monitor the use of its IT services and systems to:

- Maintain the integrity of its systems, for example to safeguard against viruses and threats
- Check that users are acting lawfully, not committing a criminal offence and complying with this policy

As part of this monitoring the Trust may collect and retain logs of such activity including email, internet records and system activity logs and audit trails. All monitoring is non-

intrusive and is undertaken in accordance with the relevant legislation and in line with the ICO Employment Practices Code.

Compliance with the aims and objectives of this policy will be monitored and reported to the Information Governance Committee.

Any breaches of policy will be reported following the appropriate HR or Risk Management Policy and Procedures. Where evidence of non-compliance is identified or suspected it will be investigated thoroughly and appropriate action taken. This may include withdrawal of access to IT services and information assets and action under the Trust disciplinary procedures.

10 References

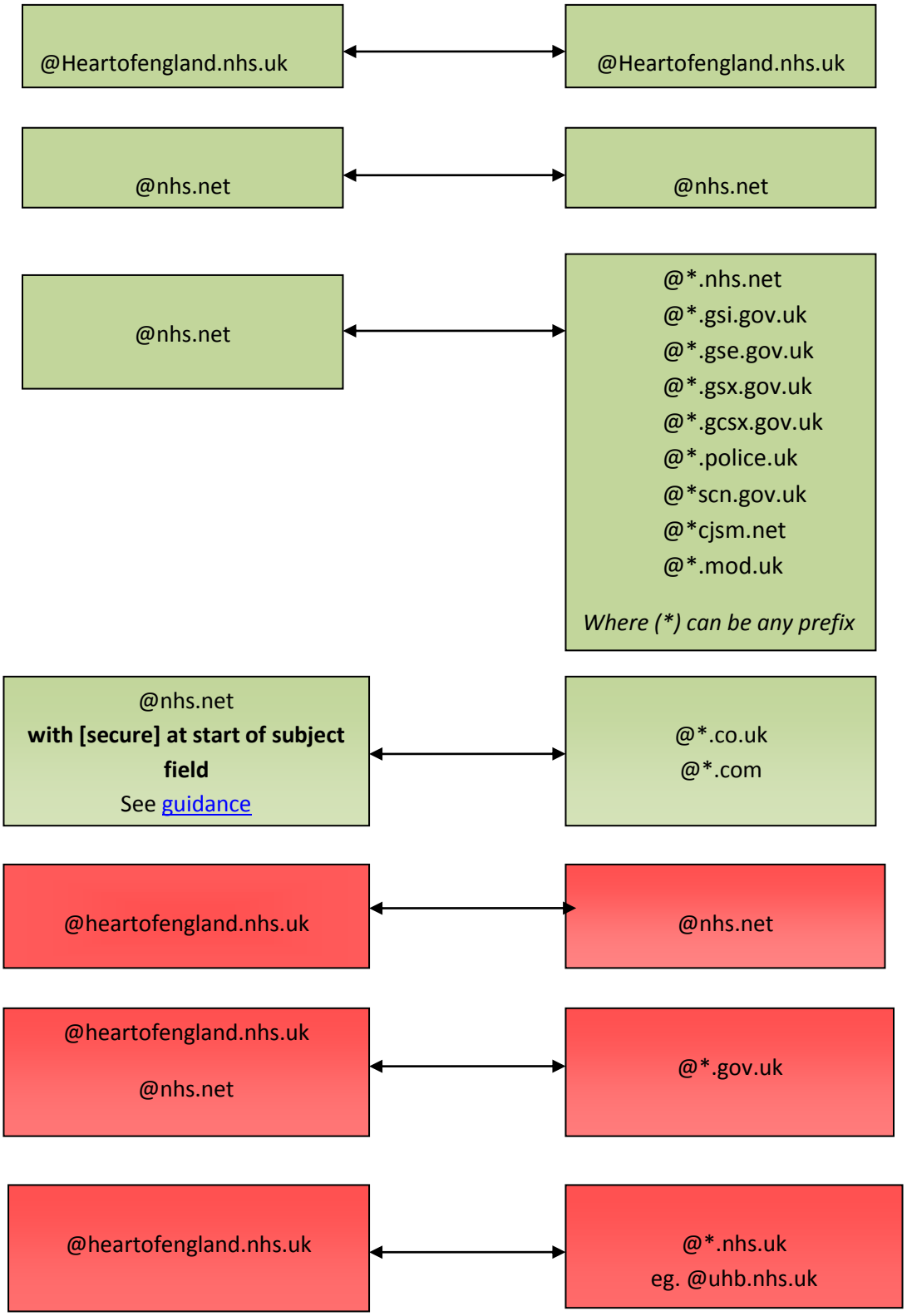
ICO Employment Practices Code

11 Attachments

Attachment 1- Secure email diagram
Attachment 2- Consultation and Ratification Checklist
Attachment 3- Equality Impact Assessment
Attachment 4- Launch and Implementation Plan

Attachment 1 - Email Security

Secure routes are Green, insecure routes are red



Attachment 2: Consultation and Ratification Checklist

Title	ICT Acceptable Use Policy

	Ratification checklist	Details
1	Is this a: *Policy & Procedure or Policy-* Policy	
2	Is this: *New or Revised* - New	
3	Format matches Policies and Procedures Template (Organisation-wide)	Y
4	Consultation with range of internal /external groups/ individuals	*Details-ICT Senior Management team and key staff, IG Committee*
5	Equality Impact Assessment completed	*Y*
6	Are there any governance or risk implications? (e.g. patient safety, clinical effectiveness, compliance with or deviation from National guidance or legislation etc)	*Y-compliance with legislation as detailed within policy*
7	Are there any operational implications?	*Y/N*
8	Are there any educational or training implications?	*Y-this will be covered through staff communications and intranet site*
9	Are there any clinical implications?	*N*
10	Are there any nursing implications?	*N*
11	Does the document have financial implications?	*N*
12	Does the document have HR implications?	*Y-this links to staff con des of conduct re acceptable use of Trust resources*

13	Is there a launch/communication/implementation plan within the document?	*Y*
14	Is there a monitoring plan within the document?	*Y*
15	Does the document have a review date in line with the Policies and Procedures Framework?	*Y*
16	Is there a named Director responsible for review of the document?	*Y*
17	Is there a named committee with clearly stated responsibility for approval monitoring and review of the document?	*Y*

Document Author / Sponsor	Ratified by (Chair of Committee or Executive Lead)
Signed	Signed
Title	Title
Date	Date

Attachment 3: Equality and Diversity - Policy Screening Checklist

Policy/Service Title: ICT Acceptable Use Policy	**Directorate: ICT**
Name of person/s auditing/developing/authoring a policy/service: Alison Baylis, Information Systems Security Specialist	
Aims/Objectives of policy/service: Ensure that users are aware of their responsibilities when accessing and using IT services and information assets and understand the associated legal and technical risks.	

Policy Content:

- For each of the following check the policy/service is sensitive to people of different age, ethnicity, gender, disability, religion or belief, and sexual orientation?
- The checklists below will help you to see any strengths and/or highlight improvements required to ensure that the policy/service is compliant with equality legislation.

1. Check for DIRECT discrimination against any group of SERVICE USERS:

Question: Does your policy/service contain any statements/functions which may exclude people from using the services who otherwise meet the criteria under the grounds of:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
1.1	Age?		**X**				
1.2	Gender re-assignment?		**X**				
1.3	Disability?		**X**				
1.4	Race or Ethnicity?		**X**				
1.5	Religion or belief (including lack of belief)?		**X**				
1.6	Sex?		**X**				
1.7	Sexual Orientation?		**X**				
1.8	Marriage & Civil partnership?		**X**				
1.9	Pregnancy & Maternity?		**X**				

If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.

2. Check for INDIRECT discrimination against any group of SERVICE USERS:							
Question: Does your policy/service contain any statements/functions which may exclude people from using the services under the grounds of:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
2.1	Age?		**X**				
2.2	Gender re-assignment?		**X**				
2.3	Disability?		**X**				
2.4	Race or Ethnicity?		**X**				
2.5	Religion or belief (including lack of belief)?		**X**				
2.6	Sex?		**X**				
2.7	Sexual Orientation?		**X**				
2.8	Marriage & Civil partnership?		**X**				
2.9	Pregnancy & Maternity?		**X**				
If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.							
TOTAL NUMBER OF ITEMS ANSWERED 'YES' INDICATING DIRECT DISCRIMINATION =							
3. Check for DIRECT discrimination against any group relating to EMPLOYEES:							
Question: Does your policy/service contain any statements which may exclude employees from implementing the service/policy under the grounds of:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
3.1	Age?		**X**				
3.2	Gender re-assignment?		**X**				
3.3	Disability?		**X**				
3.4	Race or Ethnicity?		**X**				
3.5	Religion or belief (including lack of belief)?		**X**				
3.6	Sex?		**X**				
3.7	Sexual Orientation?		**X**				

3.8	Marriage & Civil partnership?		**X**				
3.9	Pregnancy & Maternity?		**X**				
If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.							
4. Check for INDIRECT discrimination against any group relating to EMPLOYEES:							
Question: Does your policy/service contain any conditions or requirements which are applied equally to everyone, but disadvantage particular persons' because they cannot comply due to:		**Response**		**Action required**		**Resource implication**	
		Yes	**No**	**Yes**	**No**	**Yes**	**No**
4.1	Age?		**X**				
4.2	Gender re-assignment?		**X**				
4.3	Disability?		**X**				
4.4	Race or Ethnicity?		**X**				
4.5	Religion or belief (including lack of belief)?		**X**				
4.6	Sex?		**X**				
4.7	Sexual Orientation?		**X**				
4.8	Marriage & Civil partnership?		**X**				
4.9	Pregnancy & Maternity?		**X**				
If yes is answered to any of the above items the policy/service may be considered discriminatory and requires review and further work to ensure compliance with legislation.							
TOTAL NUMBER OF ITEMS ANSWERED 'YES' INDICATING INDIRECT DISCRIMINATION =							

Signatures of authors / auditors: **Date of signing:**

Equality Action Plan/Report

Directorate:

Service/Policy:

Responsible Manager:

Name of Person Developing the Action Plan:

Consultation Group(s):

Review Date:

The above service/policy has been reviewed and the following actions identified and prioritised.

All identified actions must be completed by: _____

Action:	**Lead:**	**Timescale:**
Rewriting policies or procedures		
Stopping or introducing a new policy or service		
Improve /increased consultation		
A different approach to how that service is managed or delivered		

Increase in partnership working		
Monitoring		
Training/Awareness Raising/Learning		
Positive action		
Reviewing supplier profiles/procurement arrangements		
A rethink as to how things are publicised		
Review date of policy/service and EIA: this information will form part of the Governance Performance Reviews		
If risk identified, add to risk register. Complete an Incident Form where appropriate.		

When completed please return this action plan to the Trust Equality and Diversity Lead; Pamela Chandler or Jane Turvey. The plan will form part of the quarterly Governance Performance Reviews.

Signed by Responsible Manager: Date:

Attachment 4: Launch and Implementation Plan

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

Action	***Who***	***When***	***How***
Identify key users / policy writers	Information Systems Security Specialist	December 2015	
Present Policy to key user groups	Information Systems Security Specialist	January 2016	
Add to Policies and Procedures intranet page / document management system.	ICT Gatekeeper	When approved	
Offer awareness training / incorporate within existing training programmes	Information Systems Security Specialist	When approved	
Circulation of document(electronic)	Information Systems Security Specialist	When approved	