Trust Policy	NHS Worcestershire

Internet and Email Policy v08

Department / Service:	ICT
Originator:	Deputy Director of ICT Updated by Worcestershire NHS and IT Security Leads
Accountable Director:	Organisation Director of ICT or relevant lead
Approved by:	Information Governance Steering Group Trust Management Committee
Date of approval:	16/11/2015 by Worcestershire CCGs IG Steering Group
First Revision Due:	TBC
Target Organisations:	Worcestershire NHS Organisations and all users of the WHITS Network
Target Departments	All
Target staff categories	All

Policy Overview:

This policy provides guidance on the secure management and use of the Internet and the Organisation Email facility used by employees within Worcestershire NHS Organisations, at the time of writing this included:-

- Worcestershire Acute NHS Trust
- Worcestershire Health & Care Trust
- South Worcestershire CCG
- Redditch & Bromsgrove CCG
- Wyre Forest CCG

Included organisations are subject to change.

The purpose of the policy is to provide a balance between security and ease of use, and to take full account of NHS guidance and legislation.

Latest Amendments to this policy:

Amendments include:

- Appendix 3 split to prior / after NHS Mail migration (v08)
- Appendix headings updated (v08)
- Numerous grammatical changes (v08)
- Removed GP Practice reference (V07)
- Update into new policy format (v07)
- Updates around the changes for WHICTS to Computacenter (v07)

Contents page:

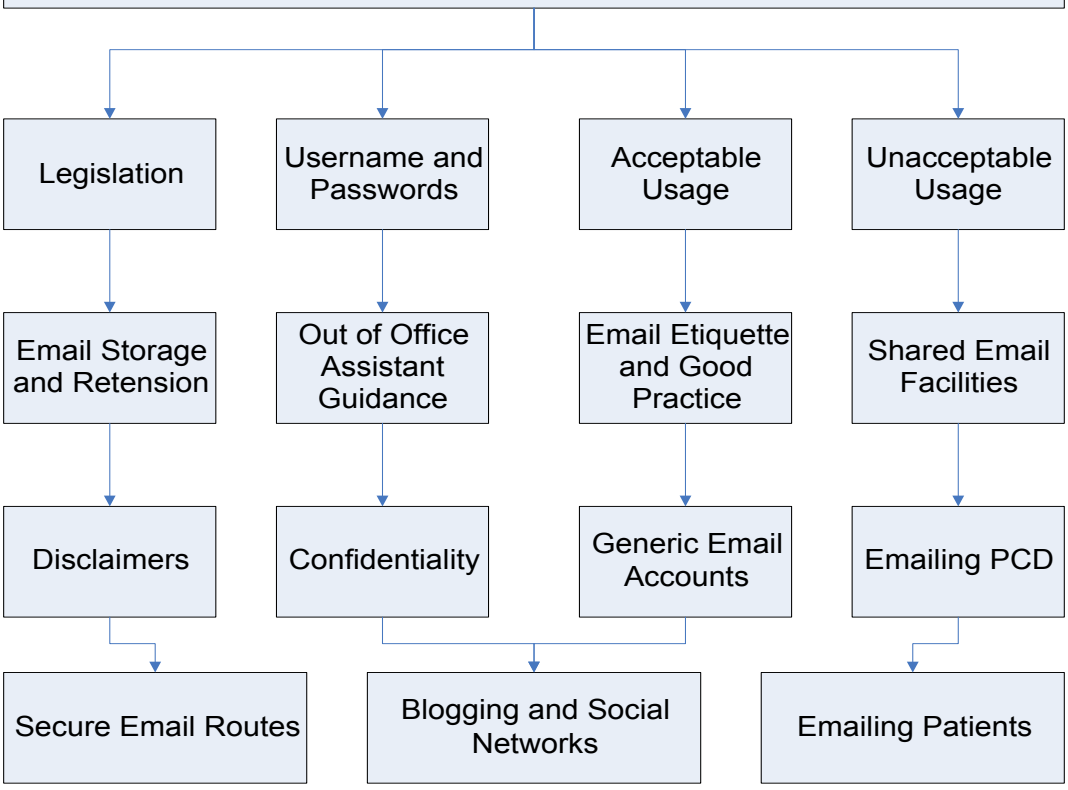
Quick Reference Guide

Internet and Email Policy

This policy provides guidance on the secure management and use of the Internet and the Organisation Email facility used by employees within Worcestershire NHS Organisations

This policy applies to all full time and part time employees, non-executive directors, contracted third parties (including agency staff), students/trainees and other staff on placement and includes the use of mobile devices

Details or Guidance in the following areas are included in this policy



1. Introduction

This policy provides guidance on the secure management and use of the Internet and the Organisation Email facility used by employees within Worcestershire NHS Organisations. The purpose of the policy is to provide a balance between security and ease of use, and to take full account of NHS guidance and legislation. If any user disregards the rules set out in this Policy, the user will be fully liable and may be subject to disciplinary action by their employing Organisation.

2. Scope of this document

This policy applies to all full time and part time employees, non-executive directors, contracted third parties (including agency staff), students/trainees and other staff on placement and includes the use of mobile devices.

Out of scope of this policy are members of the public and patients as they are not permitted to use the WHITS network.

3. Definitions

DH	Department of Health
ICT	Information & Communication Technology
IG	Information Governance
IM&T	Information Management & Technology
NHS	National Health Service
NHSCFS	NHS Counter Fraud Services
PC	Personal Computer
PCD	Personal Confidential Data
SIC	Statement of Internal Control
SIRI	Serious Incident Requiring Investigation
SIRO	Senior Information Risk Owner
WHITS Network	The name of the network used within Worcestershire NHS
Worcestershire NHS	Inclusive term of all organisations covered by Computacenter
Computacenter	IT support Provider

4. Responsibility and Duties

4.1 Computacenter

In supplying the user with a network and Email/Internet account Computacenter must ensure that there are systems and procedures in place to prevent or identify breaches of security and means of taking action against the offending parties.

Computacenter will:

- Ensure that there are formal request procedures to set up users with network and associated Email/Internet accounts.
- Use filtering and content management tools to monitor Internet usage and inbound/outbound emails to ensure security of the WHITS network system.
- Quarantine emails that are a potential threat or are of such a composition that they are deemed to be offensive or of a malicious nature.

- Ensure that any inappropriate use will be identified and reported to the appropriate line manager, IG Lead Manager, Caldicott Guardian and/or Human Resources.
- Ensure that the Email folders stored on the network are backed up on a daily basis.
- Implement and maintain anti-virus software on servers, PCs and laptops
- Ensure that access to certain websites may be restricted based on Organisational requirements

Computacenter will not:

- Routinely monitor individual users Email or Internet activity.

4.2 Worcestershire NHS Responsibilities

Ensure that all staff has access to training in the use of the Internet or Email where appropriate. This is the responsibility of individual organisations and their local ICT team.

Take all reasonable steps to ensure that all staff using the Internet and Email are aware of policies, protocols, procedures and legal obligations relating to the use of Internet and Email. This will be done through induction and mandatory update training. This is the responsibility of individual organisations and their local ICT team.

Where appropriate, disclose evidence of any member of staff contravening the law or professional standards to the police and/or regulatory bodies, including the NHS Counter Fraud Services (NHSCFS). Where relevant the local ICT or IG teams may be required to liaise with the overall ICT provider, who at the time of writing was Computacenter.

Supply or provide access to Trust policy and inform Computacenter of changes to policy.

4.3 User Responsibility

Failure to comply with this policy could result in the individual or the Organisation being prosecuted under the regulations listed in section 9.

Worcestershire NHS Organisations consider the Internet and Email to be an important means of communication. Therefore users must adhere to the following guidelines.

5. Internet and Email Policy Detail

5.1 Purpose

The purpose of this policy is to ensure the proper use of the Organisation's Internet and Email system and make users aware of what the Organisation deems as acceptable and unacceptable use. By following the guidelines in this policy, the users can minimise the legal risks involved in the use of Internet and Email. If any user disregards the rules set out in this policy, the user will be fully liable and may be subject to disciplinary action by the Organisation.

5.2 Objective

The objective of this policy is to ensure the security of the Internet and Email systems. To do this the Organisation will:

- Ensure Availability - Ensure that the Internet and Email systems are available for users. Overall provision of "core" software systems and the availability are the responsibility of the overall ICT provider, who at the time of writing was Computacenter.

- Preserve Integrity - Protect the Internet and Email systems from unauthorised or accidental modification ensuring the accuracy and completeness of the Organisation's assets. Overall provision of software protection and network configuration is the responsibility of the overall ICT provider, who at the time of writing was Computacenter.
- Preserve Confidentiality - Protect assets against unauthorised disclosure. Overall provision of software enabling support for confidentiality is the responsibility of the overall ICT provider, who at the time of writing was Computacenter.

5.3 Associated Document Framework

Document Title	Content	Review period
Internet and Email Access Policy	Principles	2 Years
User Responsibility Declaration	Statement	2 Years
Information Security Policies & Procedures ▪ Access Control ▪ Anti-Virus ▪ Back-Up ▪ Business Continuity ▪ Equipment Disposal ▪ Information Security ▪ Mobile Devices ▪ Network Security ▪ Forensic Readiness ▪ NHSmail	Requirements	2 Years
Organisation Policies & Procedures ▪ Code of Conduct in Respect of Confidentiality ▪ Data Protection ▪ Disciplinary ▪ Freedom of Information ▪ Home Working ▪ Incident Reporting ▪ Information Governance ▪ Information Risk ▪ Records Management ▪ Safe Haven	Requirements	As per Organisation requirements

5.4 Legislation

Worcestershire NHS is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of Worcestershire NHS Organisations, who may be held personally accountable for any breaches of Internet or Email security for which they may be held responsible, failure to comply could result in the individual or the Organisation being prosecuted. Worcestershire NHS Organisations shall comply with the legislation, detailed in section 9, and other legislation as appropriate.

5.5 User names and passwords

Staff should be aware they are fully responsible for the security of their individual login and password, so must not share them with anyone. If a breach of security is recorded under a member of staff's login then they will be liable.

Staff should ensure that they log out completely and not leave open sessions unattended. Should staff discover an open session they should log out and commence their own.

The user logged in at a computer will be considered to be the author of any message sent from that computer.

The user logged in at a computer will be considered to be the person browsing the Internet.

5.6 Acceptable Usage

- To access Internet and Email for personal use so long as this does not interfere with work, or the work environment, and if it does not breach locally defined policies and procedures or "Unacceptable Usage" rules below.
- Personal use is at the discretion of the Organisation, and if demands at particular times of the day become excessive (i.e. lunchtime), and performance of the network suffers as a result, personal use may have to be reduced or removed.
- To access research material and other information relevant to your work
- Staff should be aware that the security of sites visited and of their personal details (name, address, financial information etc.) cannot be guaranteed since temporary files and internet page history records are often automatically retained by PCs.
- For further information contact the IT Helpdesk.

5.7 Unacceptable Usage – Email

Creating or transmitting "junk-mail" or "spam", this means unsolicited commercial web mail, chain letters or advertisements e.g. circulating emails promoting your own business. There are thousands of Email hoaxes moving around the Internet at any given time. These Email hoaxes cover a range of subject matter, including:

- Supposedly free giveaways in exchange for forwarding Emails.
- Bogus virus alerts.
- False appeals to help sick children.
- Pointless petitions that lead nowhere and accomplish nothing.
- Dire, and completely fictional, warnings about products, companies, government policies or coming events.

Email addresses must not be disclosed unnecessarily. Disclosing Email addresses when filling in surveys or questionnaire will/may increase the risk of receiving unwanted junk messages.

- No one should send Global emails. Contact the IT Service Desk if there is any information which needs to be distributed to a large circulation for advice on the best methods.
- Remember that all laws relating to written communication also apply to Emails and they could be presented as evidence in a court or tribunal.
- Your Emails may also be open for disclosure to anyone making a request under the Freedom of Information Act 2000 or a subject access request under the Data Protection Act 1998.
- In addition users should be aware of their responsibilities to:
    - Ensure that the identity of a recipient to whom they are sending an Email is correct.
- Any transmission of PCD to an unauthorised and/or unsecured Email system must be encrypted (see Appendix 1 for guidance on emailing PCD). A list of authorised and secure Email addresses is contained in Appendix 3. For further information on NHSmail acceptable usage please follow this link – click here
- Any use of a commercial or profit making nature, or any other form of personal financial gain.
- **Excessive personal use** for example the continual use of Email for on-going "chit chat" that interferes with the performance of your duties.

5.8 Unacceptable Usage – Internet

- Creating, downloading or transmitting (other than for properly authorised and lawful research) any obscene or indecent images, data or other material or any data capable of being converted into obscene or indecent images or material.
- Accessing Child Pornography will result in immediate reporting of the incident to the police. (THIS IS A CRIMINAL OFFENCE)
- Creating, downloading or transmission of material that is abusive or threatening to others, serves to harass or bully others or designed to cause distress or anxiety. For example any material that discriminates on the grounds of race or ethnicity, gender, sexual orientation, disability or political or religious beliefs.
- Posting of messages on Internet message boards or other similar web-based services that would/could bring the NHS into disrepute, or contravenes confidentiality requirements, such as Facebook, Twitter, Bebo and Wikipedia; for further details please refer to Appendix 4 Guidance on Blogging and Social Networking.
- Using the Internet to conduct private or freelance business for the purpose of commercial gain.
- Excessive use of the Internet for personal use e.g shopping, banking.
- Personal use of the Internet must be limited to official break times or outside working hours
- Creating, downloading or transmitting data or material that is created for the purpose of corrupting or destroying other user's data or hardware.
- Downloading (and uploading) streaming video or audio/music for entertainment purposes.
- Accessing gambling sites.

- Creating, downloading or transmitting information of a terrorist content that would otherwise draw the attention of the security agencies to accesses made from the Organisation.

- Any member of staff unintentionally connected to an inappropriate site should inform their line manager and the IT Service Desk.

- Reasonably understand copyright, trade-mark, libel, slander and public speech control laws, so that their use of the Email service does not inadvertently violate any laws which might be enforceable against the Organisation e.g. slanderous comments on “Friends Reunited”, downloading illicit music. Copyright is a piece of text which accompanies a work and expresses the rights and wishes of the owner(s), you will normally need permission to use someone else's copyright work but in certain very specific situations you may not. Copyright applies to all sorts of written and recorded materials from software and the internet to drawings and photography.
- PCD, confidential or sensitive information should not be entered on web based surveys; unless it meets encryption standards; any such requirement would need Caldicott Guardian/SIRO approval.

5.9 Email Access via NHSmail

The Organisations use the centrally funded NHSmail system to provide email services to their staff. The use of this email system is regulated by the policies and guidance of the Health and Social Care Information Centre (HSCIC). Staff are reminded that while access to the NHSmail system is available via standard internet connection, staff are liable for the control of information that is stored within their email account and access to that information.

5.10 Email storage and retention

Whilst Email is not intended to be a filing system, the archiving facilities can provide a means of meeting the retention periods as detailed in the retention and disposal schedule of the Records Management Policy. Emails should be kept if they constitute a business record, note that if the information is in a document attached to the e-mail then the attachment should be saved within the normal document management system of the department (e.g. folder in the M:\ drive). Emails which need to be retained can also be stored in this way.

5.11 Out of Office Assistant

Organisation Email offers an Out of Office service, which you are encouraged to use. This allows users to provide an automated response when away from work with a predefined message that may provide an alternative contact for any urgent issues.

5.12 Email Etiquette

Email is a powerful communication mechanism and therefore it should be used in a professional and courteous manner, in a similar vein to the written or spoken word. Take care what you write, because you do not know where copies of your Email may end up. See Appendix 2 for Good Practice Guidelines

5.13 Shared Email Facilities

Organisation Email can provide delegate access to your Emails (and Calendar) to other staff on the user’s behalf. Users should be aware that in giving permissions to someone else they are still responsible for any Emails sent on their behalf. All Emails should therefore state that they are being sent on behalf of another.

5.14 Disclaimers

All Emails should have a disclaimer attached. The following is an example which can be adapted to the relevant circumstances.

Legal Disclaimer - *"This message may contain confidential and privileged information. If you are not the intended recipient you should not disclose, copy or distribute information in this e-mail or take any action in reliance on its contents. To do so is strictly prohibited and may be unlawful. Please inform the sender that this message has gone astray before deleting it."*

5.15 Confidentiality

All users are bound by Information Governance Policies including Data Protection, Freedom of Information, Confidentiality and Information Security. Users are also bound by best practice guidance such as the Caldicott Principles and the common law duty of confidentiality. Additionally, users are not permitted to disclose confidential / sensitive information relating to any aspect of the business of the NHS.

5.16 Generic Email Accounts

Generic Email accounts require an account owner to be assigned who has overall responsibility for its maintenance, including the loading of users with delegate access. Any new account needs to be requested by logging a call with the IT Service desk

Ctrl and Click for link to IT Service Desk

A Generic Account Request Form (Appendix 6) will also need to be completed by the account owner and their approving line manager.

6. Implementation

6.1 Plan for implementation

Each Organisation's Information Governance Lead will arrange for this policy to be communicated through their appropriate channels - including all directorate managers within the Organisation, whose responsibility it will then be to ensure that all staff groups within their area are directed to this policy.

6.2 Dissemination

This policy will be available on the Organisation's Intranet and circulated via Organisational Briefs/Newsletters.

6.3 Training and awareness

This policy will also be included, along with the Information Security Policy, as a requirement for any new staff member to sign up to via the User Declaration. Any key amendments to the Policy will be notified to each Organisation for communication to staff groups. Staff are also required to complete mandatory IG training annually.

7. Monitoring and compliance

The table below should help to detail the 'Who, What, Where and How' for the monitoring of this Policy.

Page/ Section of Key Document	Key control	Checks to be carried out to confirm compliance with the Policy	How often the check will be carried out	Responsible for carrying out the check	Results of check reported to: *(Responsible for also ensuring actions are developed to address any areas of non-compliance)*	Frequency of reporting
	WHAT?	**HOW?**	**WHEN?**	**WHO?**	**WHERE?**	**WHEN?**
Page 4	Breaches in policy and incidents will be identified and reported.	Initially logged as a call via the Service Desk for evaluation and, where appropriate, an Incident being raised and investigated as per each Organisation's guidelines.	Whenever a breach in Policy or an incident occurs	Investigating officer	Reported in line with Organisation Policy through IG leads and IGSG; where appropriate being escalated in line with SIRI guidelines.	Low level breaches and Incidents will be reviewed at Organisation's IGSG 4 times a year. Serious incidents will also follow this process and are additionally included in the individual Organisation's SIC and annual report, in line with HSCIC SIRI guidance.

8. Policy Review

This policy will be reviewed every 2 years, or earlier if appropriate, to take into account any changes to legislation that may occur, and/or guidance from the Department of Health, the NHS Chief Executive and/or the Information Commissioners Office.

9. References

References	Year
Access to Health Records Act	1990
Caldicott Principles	
Care Quality Commission	2009
Common Law Duty of Confidentiality	
Computer Misuse Act	1990
Confidentiality: NHS Code of Practice	2003
Copyright, Designs and Patents Act	1988
Criminal Justice and Public Order Act	1994
Data Protection Act/ Processing of Sensitive Personal Data Order	1998/2000
Electronic Communications Act	2000
Freedom of Information Act	2000
Health and Safety at Work Act	1974
Health and Social Care Act	2012
HSCIC Information Governance Toolkit	
Human Rights Act	1998
Information Security Management: NHS Code of Practice - DH	2007
Interception Of Communications Act	1985
ISO/IEC 27001 Information Security Management Standard	2005
Records Management: NHS Code of Practice	2006
Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents (SIRI)	2013
Regulation of Investigatory Powers	2000
Trade Mark Act	1994

10. Background

10.1 Equality requirements

None - equality assessment Supporting Document 1

10.2 Financial risk assessment

None - financial risk assessment Supporting Document 2

10.3 Consultation

The following stakeholders have been consulted during the production of this policy:

- Worcestershire Acute ICT Service Delivery Manager
- Information Governance Groups at Organisation and County Level
- Computacenter Information Security Lead

Contribution List

This key document has been circulated to the following individuals for consultation;

Designation
Worcestershire Acute ICT Service Delivery Manager
Information Governance Groups at Organisation and County Level
Computacenter Information Security Lead
Worcestershire Acute Director of Asset Management and ICT
Worcestershire Acute Chief Medical Officer/Deputy – Caldicott Guardian

This key document has been circulated to the chair(s) of the following committee's for comments;

Committee
Information Governance Steering Group
Trust Management Committee/Relevant Organisational Committee

10.4 Approval Process

This Policy will be approved by the relevant Committee bi-annually.

10.5 Version Control

This section should contain a list of key amendments made to this document each time it is reviewed.

Date	Amendment	By
Jun 2010	Miscellaneous, Secure Email diagram update & Blogging and Social Networking appendix	R King
Oct 2011	Update secure Email diagram	R King
Oct 2011	Update section about Email usage	R King
Jul 2012	Patients emailing services Appendix & change to Accountable Director, format & monitoring table	R King
Aug 2013	Format update, including monitoring table, and change the term Trust to Organisation	R King
Jun 2015	Amendments include: Update into new policy format Updates around the changes for WHICTS to Computacenter Updates for Worcestershire Local Health to Worcestershire NHS Inclusion of details on NHSmail and secure transfer of information Inclusion of Generic Email Request From	IT Service Delivery Manager, IG leads Countywide, Computacenter

========== End of Main Document ==========

Appendix 1 Emailing Person Confidential Data (PCD)

Do not email PCD unless absolutely necessary and as per relevant Organisations procedures, ensuring data mapping requirements are fulfilled. For patient information the NHS number should ideally be used as a means of identification, where appropriate bracketing the person's initials to confirm identity.

PCD should only be emailed if it is:

(A) Emailed by NHSmail where sender and recipient addresses **both** end in nhs.net
(B) Or to the following trusted domains form nhs.net

Department	Domains
Central Government	*.gsi.gov.uk *.gse.gov.uk *.gsx.gov.uk Note that @orgname.gov.uk is not secure.
Police & Criminal Justice	*.pnn.police.uk *.scn.gov.uk *.cjsm.net
Local Government	*.gcsx.gov.uk
Defence	*.mod.uk

As per the NHSmail Access Policy

The full domain needs to be included in the address, security is not applied when only parts of the domain are used e.g. @worcestershire.gov.uk is not secure.

Domains prefixed with an * (wildcard) mean you can use sub domains e.g. 'fred@it.gsi.gov.uk'

Auto-forwarding from an NHSmail account can only be set up to send to the domains listed above:

(C) Alternatively, organisations may choose to implement an alternative encryption system. Guidance on this is available at HSCIC

Appendix 2: Good Practice Guidelines

1. Email Good Practice

- Log in regularly and respond to requests promptly
- Advise people when you are not available. When out of the office and not able to log into your mail account, use the tools within your system to notify others of your inability to read your mail
- Be selective about who receives your Emails, especially when using "Reply to All". Do all recipients need to see the reply?
- Use distribution lists with care – is it important that all addressees receive this Email?
- use Organisation-wide distribution lists only to communicate important business information that has genuine site-wide value
- Unless there has been explicit consent to share Email addresses use the Blind Carbon Copy, Bcc, option; this is particularly relevant when emailing patients, further details in Appendix 5, but may also be relevant for other external addresses.
- Check that Emails are addressed to the correct recipient when using a Global Address List.
- Check the Email before despatch. Once you have clicked the SEND button the Email cannot be retrieved once opened
- Use discretion when forwarding a long Email message to group addresses or distribution lists
- Place large attachments in a shared location (where applicable) and then send the path to the file via the Email
- Print only essential Mail
- Request an Email delivery receipt
- Request a read receipt, using message options, only on time critical mail
- Any requirement to save personal mail should be done so in a folder marked Personal

2. Email Etiquette

- Sign off with your name, Organisation and contact details
- Use the subject field with a few short descriptive words to indicate the contents when sending Emails. It will assist the recipient in prioritising opening of Emails and aids future retrieval of opened messages
- Type your messages in lower case. Using capital letters is considered aggressive
- Be careful about content. Email is easily forwarded. Do not write something in an Email that you would not write in a letter or say to someone face to face
- Maintain the conventions normally used in sending a letter by post. If you usually address someone as "Dr. Smith", do the same in Email. Emails carry the same etiquette as traditional communication; they also carry the authority of the sender!

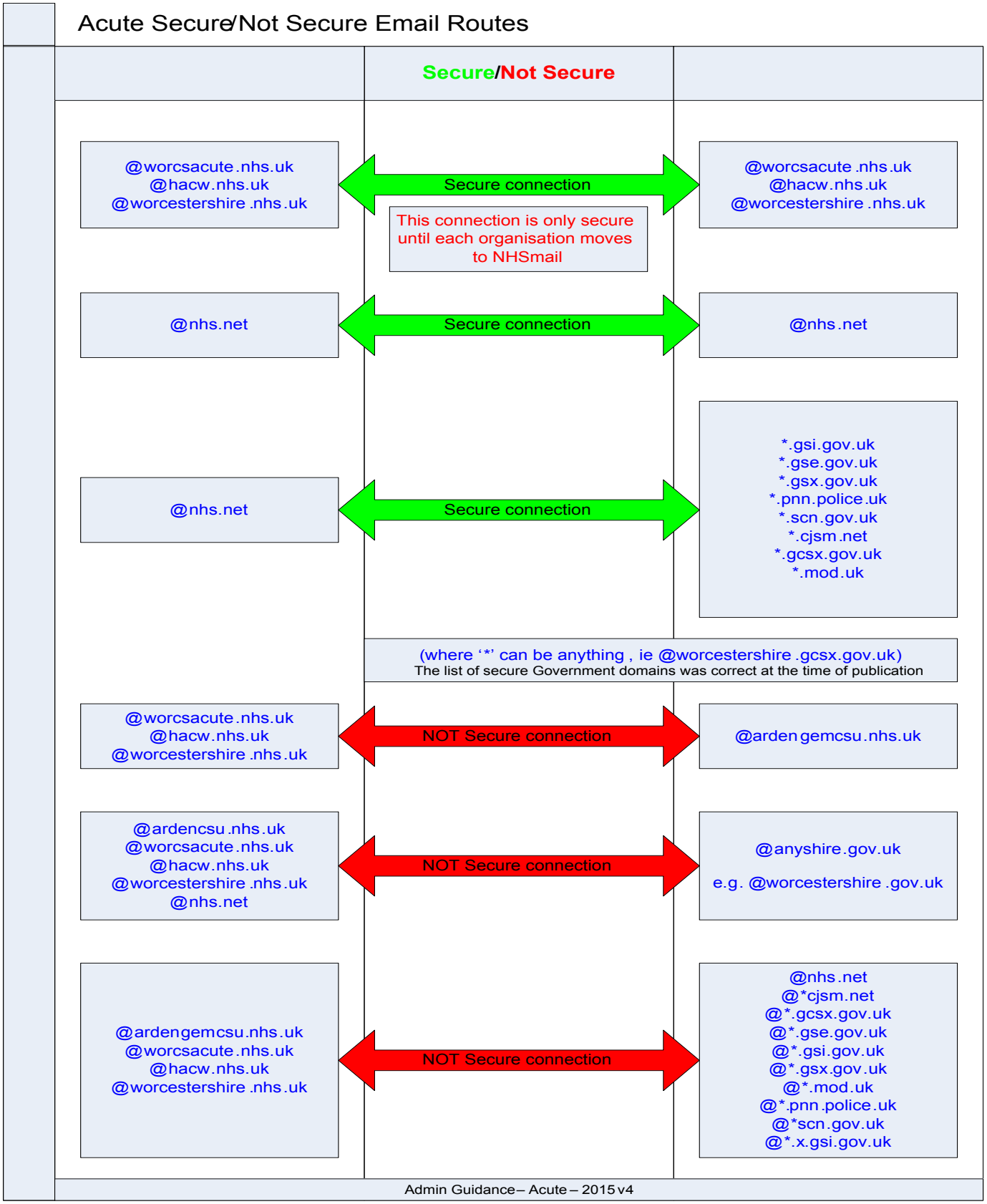
3. Email Housekeeping

- Ensure that when the size of a mailbox approaches maximum storage limit set on your server, items are moved to a folder
- Keep the amount of Email in your inbox to a minimum. Delete Emails after reading, response or action, ensuring Deleted Items is emptied regularly. Saving messages uses valuable disk space
- Review saved Emails every month and delete the ones no longer required. If there is an Email that may be required in the future, it should be archived.

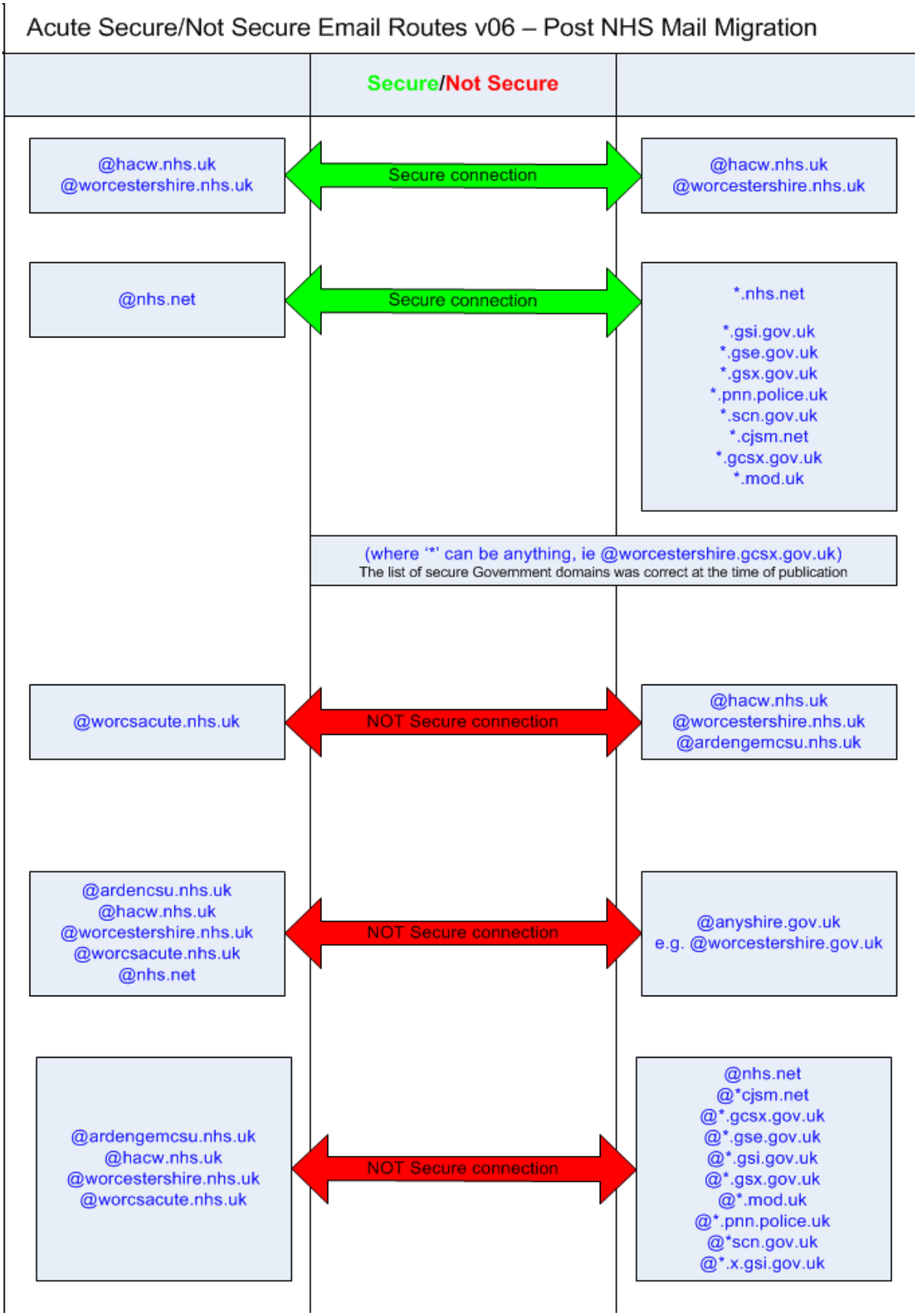
4. Issues to Avoid – Don't

- Be caught out by the speed of Email. Do not act impetuously. Is your first reaction the one you want the recipient to receive?
- Share your Email password or use other people's account to send your messages
- Send a mass mailing circular via Email
- Send Emails that may be misconstrued by the recipients
- Verbally attack in electronic form
- Send Email in upper case, this is the equivalent of shouting in someone's ear
- Send to too many people just because you can!
- Send large attachments by Email. If you believe that most recipients will print the document, try to use another method of sending the hard copy
- Send executable attachments unless essential – some intranets prohibit downloading them as Executable files cause a computer to perform tasks as opposed to a file that only contains data, so carry a higher risk of viruses

Appendix 3a: Secure Email Diagram Prior to NHS Mail Migration



Appendix 3b: Secure Email Diagram Post NHS Mail Migration



Appendix 4:

Department of Health Blogging and Social Network Guidance document from December 2009

Introduction

This Information Governance (IG) guidance provides NHS Organisations with a general awareness of the associated risks of blogging and social networking that may potentially affect the effectiveness of local services.

Terms used:

Blogging is using a public website to write an on-line diary (known as a blog) sharing thoughts and opinions on various subjects. The word blog is derived from the phrase weB LOG. Examples of blogging websites include Twitter.com and Blogging.com.

Social networking is the use of interactive web based sites that mimic some of the interactions that occur between people in life. Examples include Facebook.com and Linkedin.com.

Why are Blogging and Social networking an Information Governance issue?
The use of blogging and social networking websites by an NHS Organisation's employees can expose that Organisation to information risks, even where these sites are not accessed directly from work. Whilst there is nothing new about the information risks, what has changed is the availability of high capacity broadband, the popularity of Web2.0 sites and the rapid growth of internet enabled devices such as mobile phones, blackberries etc. This has resulted in significant awareness and uptake of these websites from home, from work and when mobile.

What are the potential dangers to the Organisation of using blogging and social networking?

A range of potential threats exist that Organisations should be aware of:

- Unauthorised disclosure of business information and potential confidentiality breach
- Blogging and social networking sites provide an easy means for information to leak from an Organisation, either maliciously or otherwise. Once loaded to a site, Organisational information enters the public domain and may be processed and stored anywhere globally. In short, Organisational control is lost and reputational damage can occur.
- Malicious attack associated with identity theft
- People often place a large amount of personal information on social networking sites, including details about their nationality, ethnic origin, religion, addresses, date of birth, telephone contact numbers and interests. This information may be of use to criminals who are seeking to steal identities or who may use the information for social engineering purposes.
- Legal liabilities from defamatory postings by employees
- When a user registers with a site they typically have to indicate their acceptance of the site's terms and conditions. These can be several pages long and contain difficult to read legal language. Such terms and conditions may give the site 'ownership' and 'third party disclosure' rights over content placed on the site, and could create possible liabilities for Organisations that allow their employees to use them. For example, where a user is registering on a site from a PC within the Organisation, it may be assumed that the user is acting on behalf of the Organisation and any libellous or derogatory comments may result in legal action. In addition, information being hosted by the website may be subject to other legal jurisdiction overseas and may be very difficult to correct or remove.
- Reputational damage
- Ill-considered or unjustified comments left on sites may adversely affect public opinion toward an individual or Organisation. This can lead to a change in social or business status with a danger of consequential impacts.

- Malicious code targeting social networking users causing virus infections and consequential damage

- Sites may encourage or require the download and installation of additional code in order to maximise the site's functionality and potential values. Where sites have weak or ineffective security controls it may be possible for code to be changed to contain malicious content such as Viruses and Trojans, or to trigger unintended actions such as Phishing.
- Systems overload from heavy use of sites with implications of degraded services and non-productive activities
- Sites can pose threats to an Organisation's information infrastructure. Particularly as the use of rich media (such as video and audio) becomes the norm in such sites, the bandwidth consumption generated by these sites can be significant and they have the potential to be the biggest bandwidth consumers within an Organisation.
- Intimidation of employees from inappropriate use of sites leading to investigations

How might the Organisation respond to these risks?

Whilst there are technical controls that could be applied the main defence against threats associated with blogging and social networking is awareness related.

Actions that may be considered by NHS Organisations include:

- Deploying technical controls to block or control permitted website usage;
- Revising and updating Organisational policies to include acceptable use of blogging and social networking sites. Policies and standards should be clear about the acceptability of accessing sites during working hours and from the Organisation's internet connected devices e.g. PCs, mobile phones etc. The consequences of non-compliance with Organisational policy should also be clear;
- Educating users about the potential business risks and impacts associated with blogging and social networking. Raising user awareness is an essential partner to the Organisation's policy and standards and should ensure that the potential dangers are known to employees who may use such sites. This will also help employees in their safe use of such services when at home.

Avoiding problems with blogging and social networking sites

A number of checks may be applied that will help NHS Organisations and their employees avoid problems:

A. Verify if the Organisation has a relevant policy and the extent to which this applies

B. Ensure that Social Networking and Blogging risks are considered within the overall approach to information risk assessment and management

C. When registering with a website, understand what you are signing up to and importantly what security and confidentially claims and undertakings exist

D. Watch for add-ons i.e. additional features or applications that change the terms and conditions of what you have signed up for, or that may require changes to the security settings of your devices

E. Withhold personal details that you do not want to be made public

F. Avoid loading work related information to blogging or social networking sites

G. Examine carefully any Email coming from social networking sites or contacts as these may be unreliable containing malicious code or be spoofed to look as though they are authentic

Appendix 5: Guidance around patients emailing the Organisation

If your service/department uses Email as a means of contacting patients, then you have a duty to inform your patients that the information contained within the Email will not be confidential or secure and can potentially be intercepted. This is a requirement of the Data Protection Act 1998 and the NHS Code of Confidentiality 2006.

Patients should be informed:

- Exactly why their information is being collected and the ways in which their information is used. Please refer to the Organisation leaflet/poster – 'Your Information: What You Need to Know'.
- The confidentiality and security of the information in the Email cannot be guaranteed whilst in transit and that an Email should contain the minimum amount of personal information required to identify them.
- The Organisation has no control over, or responsibility for, an Email stored by a patient's own Email Service Provider e.g. Hotmail; noting that personal Email accounts are vulnerable to security breaches.
- That any agreement to share their Email address with fellow patients effectively puts their Email address in the public domain, so the Organisation no longer maintains control over who it is shared with.

Staff should also be aware that:

- The actual identity of an individual sending or receiving an Email cannot always be guaranteed; please ensure that the patient's Email address has been confirmed and is periodically verified.
- That a register needs to be maintained of Email addresses being used so that on receipt of a request to remove details this can be done efficiently and that any agreement to share Email addresses with fellow patients is recorded.
- Any requirement to send information to more than one patient in a single Email should be done via the Blind Carbon Copy, Bcc, option; unless there has been explicit consent to share Email addresses. This is of particular relevance if the Organisation holds patients Email addresses in a distribution list.
- When emailing a patient an additional disclaimer should be used as well as the standard, automated, Organisation Email disclaimer. Please see an example disclaimer below.
- Where a member of staff/service/department Email is published on the Internet that is it accompanied with a disclaimer. Please see an example disclaimer below.

Suggested additional disclaimer/footer/signature:

Please be aware that the confidentiality and security of any information exchanged via Email cannot be guaranteed and that by signing up to this service you are aware of and acknowledge the associated risks. Make sure that you always use the minimum amount of personal information needed to identify yourself and/or others (*where appropriate service to specify*). The Organisation has no control, or responsibility, over personal information stored by a person's own Email Service Provider. Any personal information that is processed by the Organisation will be done so in accordance with the Data Protection Act 1998.

Appendix 6: Request for a Generic E-Mail Account

Generic E-Mail accounts allow more than one user to access an account; they should only be used if there is not a requirement to trace activity back to an individual.
Generic accounts must have an Owner assigned; this is to be the person who takes overall control and responsibility for the account. This form needs to be completed, when requesting a new generic account or reassigning ownership, by the account owner.
Requests will be considered providing the necessary control measures are in place:

Owner responsibilities
The account owner is responsible for:

- Co-ordinating the request for the generic account and obtaining the relevant line manager's authorisation.
- Deciding controlling and maintaining who has access to the generic account; this means setting up the relevant personnel with delegate access.
- Ensuring a log is maintained and retained of who has access to the Generic account
- Ensure WHITS are kept informed of changes in requirement to the generic account by the account owner logging a support call, particularly if the owner needs to be changed or the account is no longer required. Please note a new Request for a Generic Account form will need to be completed for the new named owner.
- Ensuring any use of generic email accounts for the sending/receiving of Person Identifiable Data (PCD), confidential or sensitive information (PCD for the purposes of this document) is done securely, as detailed in the secure email diagram, that Caldicott approval has been obtained for any PCD that leaves the trust and that the Code of Confidentiality, available from the Trust's Intranet, is adhered to.
- Ensure the Information Security, Internet and E-Mail and any other relevant trust policies are adhered to.

Generic Account Agreement

This Generic E-Mail Account Request must be signed by the account owner, their line manager and where appropriate the Caldicott Guardian - this can be done electronically, providing it is sent from their respective mailboxes for audit purposes.

PRINT NAME & SIGNATURE:	
JOB TITLE:	
DEPARTMENT&LOCATION:	
CONTACT TELEPHONE NUMBER:	
DATE:	
Will PCD be leaving the Trust, if so please specify?	

I Agree to the responsibilities as outlined above and:

- Are aware that the very nature of a generic account means activity cannot be attributed to an individual, thus losing the audit ability of records. Generic E-Mail should, wherever possible, be used for receiving mail and that any replies are made from an individual's mailbox.
- Failure to comply with these requirements could result in the withdrawal of the account and may lead to disciplinary action.

LINE MANAGER'S NAME & SIGNATURE:	
JOB TITLE:	
DATE:	

Service Desk call number:	
Confirmation of generic email address preferred wording:	

Supporting Document 1 - Equality Impact Assessment Tool

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Does the Policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N/A	
4.	**Is the impact of the Policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**	No	
6.	**What alternatives are there to achieving the Policy/guidance without the impact?**	No	
7.	**Can we reduce the impact by taking different action?**	No	

If you have identified a potential discriminatory impact of this key document, please refer it to Assistant Manager of Human Resources, together with any suggestions as to the action required to avoid/reduce this impact.

For advice in respect of answering the above questions, please contact Assistant Manager of Human Resources.

Supporting Document 2 – Financial Impact Assessment

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	Yes/No
1.	Does the implementation of this document require any additional Capital resources	No
2.	Does the implementation of this document require additional revenue	No
3.	Does the implementation of this document require additional manpower	No
4.	Does the implementation of this document release any manpower costs through a change in practice	No
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	No
	Other comments:	None

If the response to any of the above is yes, please complete a business case and which is signed by your Finance Manager and Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval